INGENIERÍA DE TELECOMUNICACIÓN

DEPARTAMENTO DE INGENIERÍA TELEMÁTICA

PROYECTO FIN DE CARRERA

DISEÑO Y CONFIGURACIÓN DE UNA INFRAESTRUCTURA VIRTUAL CON VMWARE

Autor: Juan José Ávila Lucero
Tutor: Ignacio Soto Campos

Leganés, Octubre de 2016

"El éxito no es la victoria
sino todo lo que has peleado
por ganar"- Rafael Nadal.

"La única manera de hacer
un trabajo genial es
amar lo que haces"- Steve Jobs

Agradecimientos

Quiero agradecer con especial énfasis a mis padres por darme la educación, por formarme como persona y por darme la oportunidad de estudiar las carreras que había elegido apoyándome de forma incondicional en todas mis decisiones y animándome en los momentos duros.
A mis hermanas y amigos por darme su apoyo y cariño en todo momento.

A mi esposa Patricia y a mis hijos Lucas y Martina, que, aunque llegaron a mi vida solo a falta de la entrega del PFC me han dado alegrías y comprensión durante la realización del mismo.

A mis compañeros de Universidad, que también me acompañaron en la realización de la Ingeniería Técnica en Telecomunicación Especialidad en Sonido e Imagen en la Universidad de Extremadura y con algunos de los cuales he convivido y he compartido vivencias. Formamos una verdadera familia.

A mi tutor, Ignacio Soto Campos, por todo lo enseñado en sus asignaturas y por haberme dado la oportunidad de finalizar mis estudios realizando el proyecto fin de carrera con él.

Por último, a toda la Universidad y en especial a los profesores que me impartieron clase o prácticas durante la carrera gracias a los cuales he podido formarme como ingeniero.

Resumen

El proyecto detalla el diseño, desarrollo, implementación y configuración de una arquitectura virtual para la migración de los servicios ofrecidos por una empresa, sustentados en un parque de servidores físicos, a este entorno virtualizado. Como tecnología de virtualización se utiliza VMware. Al mismo tiempo, y como parte de esta migración, se diseña toda la arquitectura del nuevo entorno en cuanto a comunicaciones, almacenamiento, backups, entornos funcionales, administración de la plataforma y seguridad. Así mismo se analizarán cuestiones de disponibilidad y recuperación de desastres ante contingencias en la plataforma de virtualización constituida.

Palabras clave:

Arquitectura virtual, virtualización, ESXi, VMware vSphere, Alta disponibilidad, Fiber Channel, datastores, pool de recursos, recuperación de desastres, backups, seguridad.

Abstract

The project details the design, development, implementation and configuration of a virtual architecture for migration of services offered by a company, supported by a set of physical servers, to a virtualized environment. As virtualization technology we have used VMWARE. At the same time, and as part of this migration, we have designed an entire architecture of the new environment for communications, storage, backups, functional environments, management and security platform. Also, we analyse issues of scalability and disaster recovery for contingencies in platafoms of virtualization.

Keywords:

Virtual architecture, virtualization, ESXi, VMware vSphere, High Availability, Fiber Channel, datastores, resource pool, disaster recovery, backups, security.

Índice General

Tabla de contenido

1. Introducción y Objetivos 12
1.1. Motivación 12
1.2. Objetivos 13
1.3. Fases de desarrollo 13
1.4. Medios empleados 14
1.5. Estructura de la memoria 15

2. Situación inicial y ventajas de la virtualización 16
2.1. Presentación de la empresa 16
2.2. Arquitectura de virtualización 20
2.3. Ventajas de la virtualización 23
2.4. VMware frente a otras tecnologías de virtualización 25
2.5. Resumen y conclusiones 28

3. Análisis y diseño global de la arquitectura virtualización 29
3.1. Análisis y Planificación 29
3.2. Identificación Licencias VMware 31
3.3. Diseño pool de recursos arquitectura virtual 34
3.3.1. Diseño de CPU en infraestructura de VMware vSphere 34
3.3.2. Clúster de Hosts ESXi en infraestructura VMware vSphere 38
3.3.3 Diseño de la memoria RAM en infraestructura VMware vSphere 40
3.4. Diseño de los servicios de red en infraestructura VMware VSphere 42
3.5. Diseño de la red de Almacenamiento VMware vSphere 47
3.5.1. Tecnología de almacenamiento 47
3.5.2. Red SAN de la infraestructura virtual 51
3.5.3. Sistema de archivos de VMware 55

4. Implantación de la arquitectura de virtualización 58
4.1. Instalación y configuración de la red Ethernet 58
4.2. Instalación y configuración del vCenter Server 65
4.3. Instalación y configuración de los servidores físicos ESXi 74
4.4. Instalación y configuración de la red SAN Fiber Channel 77
4.4.1 Instalación y configuración switches FC 77
4.4.2. Instalación y configuración de la cabina IBM 84
4.5. Configuración de la suite VMware vSphere 5 93
4.5.1. Conexión al vCenter Server 93
4.5.2. Creación del clúster de hosts ESXi 94
4.5.3. Integración de los servidores ESXi en el vCenter Server 97
4.5.4. Virtualización de los servidores físicos actuales 110
4.5.5. Supervisión del pool de recursos de CPU y RAM 113
4.6. Resumen y conclusiones 115

5. Administración y gestión de la plataforma virtual 116
5.1. Procedimientos para la administración de la plataforma VMware 116
5.2. Procedimientos para la optimización y gestión de recursos VMWARE 124
5.2.1. Gráficos de rendimiento del vCenter Server 130

5.3. Herramientas complementarias de administración y gestión 135
5.4. Resumen y conclusiones 136

6. Copias de seguridad, recuperación de desastres y continuidad de negocio 138
6.1. Sistemas de Copias de Seguridad 138
6.2. Replicación del centro de datos 143
6.3. Protocolo de recuperación de desastres y continuidad de negocio 146
6.4. Resumen y conclusiones 154

7. Conclusiones y líneas futuras 156

8. Planificación de tareas y Presupuesto 159
8.1. Planificación de tareas 159
8.2. Presupuesto 160

9. Glosario de acrónimos y abreviaturas: 162

10. Bibliografía y referencias 167

Índice de Figuras

Figura 1: Arquitectura virtual (tomada de [1])

Figura 2: Virtualización de la CPU (tomada de [3])

Figura 3: Soluciones de computación en la nube de VMware (tomada de [1])

Figura 4: Ediciones y kits de VMware vSphere 5.0 (tomada de [7])

Figura 5: Distribución y colocación de los módulos de memoria (tomada de [27])

Figura 6: Arquitectura de red Ethernet virtual de la infraestructura

Figura 7: Arquitectura de red Ethernet física de la infraestructura virtual

Figura 8: Componentes típicos de una SAN FC (tomada de [1])

Figura 9: Arquitectura de la red SAN

Figura 10: Sistema de ficheros VMFS de VMARE (tomada de [1])

Figura 11: Configuración stack de los switches Ethernet AT8000GT/48

Figura 12: Conexiones parte trasera del switch AT8000GT/48

Figura 13: Configuración inicial del switch AT8000GT/48

Figura 14: Configuración puertos trunks switches AT8000GS/48

Figura 15: Configuración avanzada de los switches AT8000GS/48

Figura 16: Base de datos VIM_VCDB para Vcenter Server

Figura 17: DSN de 64 bits para Vcenter Server

Figura 18: Instalador VMware Vcenter

Figura 19: Creación del Datacenter de la infraestructura virtual

Figura 20: Realizando RAID con MegaRAID BIOS Config

Figura 21: Seleccionamos el RAID1 para realizar la instalación.

Figura 22: Parte frontal switch FC AT8000GS/48

Figura 23: Cabina DS3524 (tomada de [30])

Figura 24: Configuración inicial de la cabina principal DS3524

Figura 25: Configuración San Fiber Channel con canal dual (tomada de [30])

Figura 26: Configuración del almacenamiento a través del DS Storage Manager

Figura 27: Configuración final de la cabina de almacenamiento IBM DS3524

Figura 28: Asistente de creación del clúster

Figura 29: EVC con Intel® Xeon Core 2

Figura 30: Clúster con los 4 host ESXi integrados

Figura 31: Configuración predeterminada de un switch virtual estándar

Figura 32: Configuración del NIC Teaming

Figura 33: Política de seguridad seguida en cada host

Figura 34: Configuración de los grupos de puertos de las máquinas virtuales

Figura 35: Configuración de la red de gestión

Figura 36: LUN presentadas desde la cabina de almacenamiento a los ESXi

Figura 37: Adaptadores FC del host y dispositivos FC detectados

Figura 38: Característica de la licencia disponible en cada host ESXi

Figura 39: Política de seguridad seguida en cada host

Figura 40: Pool de recursos de la arquitectura virtual

Figura 41: Clúster arquitectura virtual con VMware

Figura 42: Panel de bienvenida instancia Vcenter Server

Figura 43: Estado de Hardware de un host ESXi

Figura 44: Listado(parcial) de alertas predefinidas

Figura 45: Parámetros para el control de recursos disponibles (tomada de [37])

Figura 46: CPU Ready para el ESX2

Figura 47: Uso de memoria RAM del ESX2

Figura 48: Latencia de comando del kernel y latencia de comando del dispositivo físico

Figura 49: Herramienta RVtools sobre la arquitectura virtual

Figura 50: Arquitectura de copias de seguridad

Figura 51: Modo de funcionamiento Global Mirroring (tomada de [42])

Figura 52: Arquitectura SAN con cabina DS3524 de replicación (tomada de [42])

Figura 53: RPO y RTO en un PRD

Índice de Tablas

Tabla 1: Modo Scale Up y Scale Out

Tabla 2: Máxima cantidad de memoria RAM RDIMM a instalar

Tabla 3: VLAN disponibles

Tabla 4: Funcionalidades vSphere con las tecnologías de almacenamiento (tomada de [1])

Tabla 5: Descripción VLAN

Tabla 6: Características del servidor Vcenter

Tabla 7: Características de los servidores ESX

Tabla 8: Configuración inicial de los switches FC

Tabla 9: Alias switch 1

Tabla 10: Alias switch 2

Tabla 11: Zoning switch 1

Tabla 12: Zoning switch 2

Tabla 13: Zoning completo

Tabla 14: IPs por defecto de las controladoras

Tabla 15: IPs en producción de las controladoras

Tabla 16: Arrays creados

Tabla 17: Información LUN creadas

Tabla 18: Identificación de los hosts de la SAN

Tabla 19: Políticas de programación

Tabla 20: Valores RPO/RTO en un los tres escenarios

Tabla 21: Tareas del proyecto

Tabla 22: Presupuesto final del proyecto

Capítulo 1:

1. Introducción y Objetivos

Este primer capítulo realiza la presentación de este proyecto fin de carrera haciendo un breve recorrido por la motivación que ha llevado a su realización, los objetivos del proyecto, sus fases de desarrollo, los medios con los que se ha contado para hacer el proyecto y un esquema de la memoria, que se presenta en este documento, con el fin de facilitar la tarea al lector.

1.1. Motivación

La motivación de realizar este proyecto fin de carrera es básicamente porque es una de las partes más importantes de la ocupación laboral en mi empresa en los últimos 4 años. Las tendencias del mercado, el estado actual de los servidores y todas las ventajas que proporciona la virtualización motivaron que la empresa decidiera migrar todos sus servicios actuales, desplegados sobre servidores físicos, a una nueva arquitectura virtual utilizando VMWARE. Además, se aprovechó este paso para diseñar de forma completa la arquitectura de comunicaciones y datos, los backups, las políticas de seguridad y los planes de contingencia. En este proyecto se describe con detalle el diseño e implementación de esta nueva arquitectura virtual basada en VMWARE, la migración de los servicios y la definición de las nuevas políticas para adaptarse a esta nueva arquitectura virtual.

1.2. Objetivos

El objetivo fundamental del proyecto es el diseño e implementación de una arquitectura de servidores utilizando VMware. Los servidores, virtualizados sobre una plataforma de almacenamiento, deberán ofrecer los servicios de la empresa con todas las ventajas que proporciona la virtualización e incluir los servicios actuales, sustentados sobre servidores físicos. A la hora de diseñar e implementar la solución técnica se consideraron los siguientes objetivos:

- Implementar una plataforma tolerante a fallos, tanto a nivel lógico como físico.
- Reducir el número de servidores físicos reduciendo los costes y optimizando el uso de recursos compartidos.
- Integrar la plataforma de servidores virtuales dentro de la solución de almacenamiento.
- Gestionar de forma centralizada todos los servidores virtuales.
- Implantar un entorno de alta disponibilidad.
- Implantar un sistema de backup para asegurar la recuperación de desastres y la continuidad de negocio.
- Incrementar la flexibilidad y rapidez para el despliegue de nuevos recursos necesarios para responder a demandas creadas.

1.3. Fases de desarrollo

En este apartado se van a describir las distintas fases que se han llevado a cabo para la consecución de la implantación completa del proyecto. Las fases de desarrollo llevadas a cabo son expuestas a continuación:

- Análisis y objetivos
- Diseño de la arquitectura
- Implantación de la arquitectura
- Gestión y administración de la plataforma
- Copias de seguridad, recuperación de desastres y continuidad de negocio
- Conclusiones
- Cierre del proyecto

1.4. Medios empleados

En este apartado se van a describir los medios con los que se ha contado para llevar a cabo la implantación completa del proyecto. Los medios disponibles durante el proyecto son expuestos a continuación:

- Siete servidores físicos.
- Dos cabinas de almacenamiento con 24 discos de 1 TB.
- Dos switches Ethernet.
- Dos switches Fiber Channel.
- Cableado Ethernet y cableado de Fibra LC-LC.
- Licencias de VMware vSphere Standard 5 y Vcenter Server Standard 5.
- Licencias de Backup Commvault.
- Un rack en un CPD contratado a un ISP que incluye comunicación en anillo con Fibra con otras sedes empresariales a través de una red privada virtual MPLS y con acceso a internet simétrico garantizado.
- Dos Firewall con configuración en alta disponibilidad.

1.5. Estructura de la memoria

La presente memoria está organizada en los siguientes capítulos:

Capítulo 1: Introducción y objetivos: En este capítulo se realiza la presentación del proyecto.

Capítulo 2: Situación inicial y ventajas de la virtualización: En este capítulo se presenta la situación de la empresa que motivó la implantación de la arquitectura virtual y se presenta la tecnología de virtualización.

Capítulo 3: Análisis y diseño global de la arquitectura de virtualización: En este capítulo se describen las tareas de diseño para la definición de los elementos que componen la arquitectura virtual VMware.

Capítulo 4: Implantación de la arquitectura de virtualización: En este capítulo se va a describir detalladamente el proceso de implantación del diseño de la arquitectura virtual VMware.

Capítulo 5: Administración y gestión de la plataforma virtual: En este capítulo se describen todas las tareas y procedimientos llevados a cabo para la gestión y administración de la plataforma virtual VMware.

Capítulo 6: Copias de seguridad, recuperación de desastres y continuidad de negocio: En este capítulo se describen los procedimientos para las copias de seguridad y redundancia de datos y recuperación de desastres y continuidad de negocio.

Capítulo 7: Conclusiones y líneas futuras: En este capítulo se analizan las conclusiones obtenidas al finalizar el proyecto, la situación actual de la arquitectura virtual y las acciones futuras a realizar.

Capítulo 8: Presupuesto: En este capítulo aparece el presupuesto completo para la realización del proyecto.

Capítulo 9: Glosario y abreviaturas: En este capítulo se muestra una relación de los principales acrónimos y abreviaturas utilizados.

Capítulo 10: Bibliografía y referencias: En este capítulo se presentan todas las referencias bibliográficas y referencias webs consultadas para la correcta realización del proyecto.

Capítulo 2:

2. Situación inicial y ventajas de la virtualización

En este primer apartado se va a llevar a cabo la presentación de la empresa donde se implantó la arquitectura virtual basada en VMware, la situación de partida antes de la implantación de la arquitectura virtual, y las aplicaciones y servicios que se pretenden desarrollar en la compañía a corto plazo y que motivan la citada implantación. Además, se verán las principales ventajas de la virtualización que motivan la migración, el despliegue y la implementación de nuevos servicios sobre esta tecnología y los principales motivos para utilizar VMware como tecnología de virtualización.

2.1. Presentación de la empresa

El objetivo de este proyecto es describir la solución llevaba a cabo en el año 2012 para dotar a mi empresa de una plataforma de almacenamiento y virtualización de servicios que cubra los requisitos exigidos para ofrecer de forma óptima todos los servicios tecnológicos de la empresa.

Desde hace diez años trabajo en una empresa que ofrece servicios a colegios profesionales provinciales de un determinado colectivo profesional. Los profesionales de este colectivo deben estar colegiados para poder desarrollar la profesión. En la situación de partida se ofrecían los siguientes servicios tecnológicos:

- Servicio de correo electrónico:
    - Buzones de 10 GB.
    - POP3/IMAP.
    - SMTP.
    - Acceso web y configuración clientes de correo.
    - Calendarios y contactos.

  - Gestión de usuarios y listas de distribución.
  - Servicios Antispam/Antivirus.
- Hospedaje de webs para colegios provinciales.
  - Gestión del registro del dominio.
  - DNS.
  - Bases de datos.
  - FTP.
  - Creación de discos virtuales
- Blog, foros y portales colectivo profesional.
- Sistemas de acreditación de cursos online.
- Campus de formación de cursos online.
- Acceso a Bibliotecas documentales de la profesión.
- Intranets, portales informativos y web corporativas.
- Aplicativo interno para el control y registro de entrada y salida de los documentos en papel.

Además, el parque de servidores de la empresa ofrecía también servicios internos para el funcionamiento de los puestos de trabajo de los trabajadores propios y sus actividades departamentales:

- Servidores de ficheros para la gestión de información de los puestos de trabajo de los empleados de la propia empresa.
- Servicios de Directorio Activo de Windows.
- Programa de gestión contable.
- Servicios de seguridad Firewall y antivirus.
- Telefonía IP.

En esta situación de partida también cabe incluir la gestión de todos servicios tecnológicos (TI) proporcionados internamente a la propia empresa, así como la administración y gestión de los servidores físicos que sustentaban estos servicios y los proporcionados a los colegios profesionales.

Sin embargo, en ese momento el comité directivo de mi empresa, asesorados o influenciado por el propio colectivo profesional al que daba servicio, las Administraciones Públicas y un informe de viabilidad tecnológica de nuestro propio departamento de TI, decidió dar un giro a la forma de realizar los trámites, gestiones y actividades de los colegios profesionales. Según esto, desde este comité se favoreció el nacimiento de aplicaciones de gestión de trámites electrónicos que permitieran realizar todas las funciones y procedimientos que exigían la presencia física del colegiado de forma

telemática. La introducción de esta nueva forma de gestión se vio favorecida seguramente por políticas de ahorro de costes provocados por la crisis económica existente. La acuciante crisis económica de la época favoreció la digitalización de todos los trámites con el fin del ahorro de costes. También contribuyeron a ello la publicación de algunas normativas estatales para los colectivos profesionales y Administraciones públicas como fue la Ley Ómnibus (Ley 25/2009, de 22 de diciembre). Entre los servicios y aplicativos que se pretendían implementar a partir de ese momento estaban:

- Aplicativo de Registro de profesionales del colectivo actualizable en tiempo real por los colegios provinciales a través de servicios web seguros.
- Tramitación y repositorio de receta electrónica.
- Tramitaciones colegiales mediante ventanilla única: e-gestión
- Certificados electrónicos profesionales.
- Aplicaciones para la gestión de trámites en Fundaciones del colectivo profesional.
- Oficina de promoción de empleo para el colectivo.
- Prestador de servicio de certificación mediante PKI para generar certificados digitales para el colectivo. Esto permite proporcionar acceso seguro a los aplicativos y que el intercambio de información en la realización de los trámites electrónicos disponga de confidencialidad, integridad y no repudio. Además, permite la identificación unívoca y habilitación del colegiado para el ejercicio de su profesión en el ámbito digital.
- Servicio de portafirmas para la certificación digital de los trámites telemáticos.
- Diario digital exclusivo del colectivo profesional.
- Red Social corporativa.
- Validación periódica del colegiado para el ejercicio de la profesión.
- Gestor documental de uso interno en la empresa basado en Alfresco.
- Aplicativos para la gestión y ordenación departamental.
- Gestor de soporte de incidencias.

Finalmente, se debían considerar también la evolución y adaptación de las tareas propias de administración y gestión de sistemas ante el nuevo entorno de aplicaciones y servicios a proporcionar: tareas de mantenimiento, actualización de SO, corrección de bugs y parches, sistemas de backups y replicación, resolución de incidencias, soporte, seguridad, etc.

La política seguida en la empresa hasta ese momento a nivel de sistemas era disponer de servidores independientes asociados a los servicios a desplegar, y por cada nuevo servicio a introducir

se compraba uno o varios servidores nuevos dependiendo de la criticidad del servicio y de si se quería proporcionar redundancia o alta disponibilidad al sistema. Esto originaba que nuestro Centro de Procesamiento de Datos, en adelante CPD, fuera creciendo basándose en hitos aislados, en función de las necesidades del negocio. Si había que montar una nueva base de datos X, se examinaban las distintas comparativas y se compraba el servidor más potente para esa base de datos X, del fabricante y sistema operativos indicados. Si seguidamente había que montar un servicio de Active Directory, se compraba el servidor mejor para este tipo de servicios, muy posiblemente de otro fabricante y otro sistema operativo que el anterior. Y así sucesivamente. Este tipo de crecimiento de nuestro parque de servidores provocaba que nuestro CPD llegara a un punto en el que se había vuelto inmanejable y difícilmente sostenible y administrable, debido al alto número de servidores, la dificultad para coordinar cambios en el CPD, las múltiples consolas que era necesario visualizar para conocer exactamente cómo se estaba comportando el CPD, etc. Además, para empeorar más la situación, se generaban unos costes altísimos:

- Esta política de gestión de servicios en el CPD, hacía que los recursos cada más escasos fueran el espacio, el consumo de electricidad y la refrigeración: cada máquina ocupa un espacio y consume electricidad para su alimentación y refrigeración. Además, cada vez los servidores eran más potentes y necesitaban un consumo mayor. Esto provocó la subida de precios de estos recursos en los CPD. Además, esto nos llevó a tener que realizar una migración desde un CPD que se había quedado sin recursos a otro con más recursos de reciente creación con todas las implicaciones y trastornos que eso conllevaba: interrupción de servicio, traslado de servidores, montaje y desmontaje en el antiguo y nuevo CPD, etc.
- Analizando el consumo de los recursos de nuestros servidores llegamos a la conclusión de que la utilización de recursos disponibles en los servidores físicos llegaba a máximos del 50% y se situaba en media en torno al 20%. Esto suponía que se estuvieran desperdiciando un porcentaje muy elevado del coste pagado en soporte hardware al fabricante, licencias hardware, coste de monitorización y seguridad, espacio en el bastidor del CPD, refrigeración, energía, etc. en cada servidor.
- Los costes de disponer de elementos redundantes que permitieran la continuidad de negocio y recuperación de desastres también se multiplicaban por el número de servicios a implantar.

La administración, la escalabilidad, la seguridad, el mantenimiento y aprovechamiento de los servidores era cada vez más compleja en la arquitectura física que se tenía. Con el fin de gestionar de forma más eficiente todos estos aspectos tomamos la decisión de implantar la virtualización. La

virtualización nos permite evolucionar desde el CPD tradicional, basado "en hierro", a un CPD de nueva generación, basado "en software", en el que el mejor aprovechamiento permite tratar el centro de datos como un pool de recursos compartidos que se asigna dinámicamente a las aplicaciones que lo necesiten. Este nuevo concepto de CPD nos permite centrarnos en el servicio y no en la operación, mediante la abstracción del hardware y eliminación de la gestión física de dispositivos.

2.2. Arquitectura de virtualización

La virtualización es una tecnología de software que permite simular la existencia de hardware y crear múltiples servidores virtuales bajo un servidor físico virtualizado (o un clúster) que denominaremos host (host ESXi en el caso de VMware) . La virtualización, que consolida el entorno para ejecutar las aplicaciones en máquinas virtuales, permite ejecutar más cargas de trabajo en un solo servidor físico. En la siguiente figura se muestran los elementos más importantes de una arquitectura virtual[*] [1][2]:

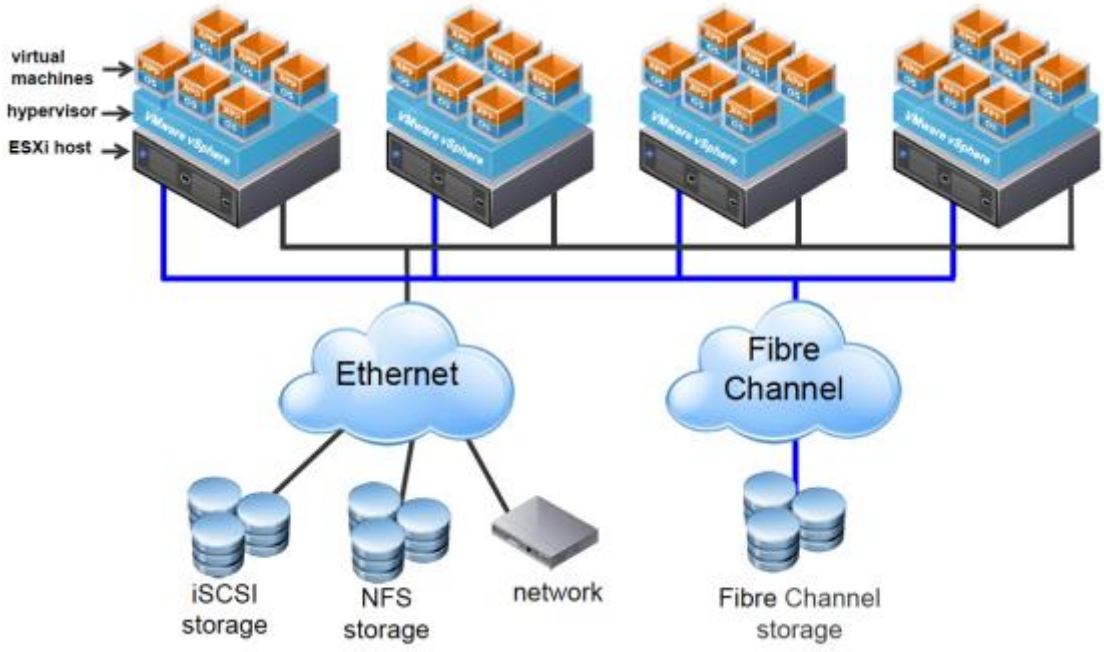


Figura 1: Arquitectura virtual (tomada de [1])

En la arquitectura física, el sistema operativo interactúa directamente con el hardware instalado: programa los procesos que se ejecutan, asigna memoria a las aplicaciones, intercambia datos

[*] La figura muestra una arquitectura virtual utilizando VMware pero los componentes serían idénticos para cualquier tecnología de virtualización.

mediante interfaces de red y lee y escribe en los dispositivos de almacenamiento conectados. En cambio, en la arquitectura virtual los recursos físicos están compartidos. De este modo, un servidor físico virtualizado interactúa con el hardware instalado mediante una capa de software llamada capa de virtualización o hipervisor*. El hipervisor proporciona dinámicamente a las máquinas virtuales los recursos de hardware físico que necesitan para funcionar. El hipervisor permite que las máquinas virtuales funcionen con cierto nivel de independencia del hardware físico subyacente. Por ejemplo, las máquinas virtuales se pueden trasladar a otro host. Además, sus discos virtuales se pueden mover de un tipo de almacenamiento a otro sin alterar su funcionamiento propio.

Una máquina virtual es un servidor creado por software que, al igual que un servidor físico, ejecuta un sistema operativo y unas aplicaciones. Cada máquina virtual contiene su propio hardware virtual con su CPU, memoria, disco duro y tarjeta de interfaz de red virtuales que aparecen como hardware físico ante el sistema operativo y las aplicaciones. Las máquinas virtuales se gestionan mediante elaborados mecanismos de control que deciden cuánto acceso puede tener cada máquina virtual al pool de recursos compartido de la plataforma virtual. Con la configuración predeterminada de asignación de recursos cada máquina virtual de un host recibe la misma proporción de los recursos disponibles.

La virtualización de procesadores (vCPU) prioriza el rendimiento y se ejecuta directamente en las CPU disponibles, siempre que sea posible. Los recursos físicos subyacentes se utilizan en la medida de lo posible, y la capa de virtualización ejecuta instrucciones solo cuando es necesario, de modo que las máquinas virtuales funcionan como si se ejecutaran directamente en una máquina física. En la siguiente figura puede verse la arquitectura de la virtualización de procesadores:

Figura 2: Virtualización de la CPU (tomada de [3])

El número de vCPU (procesadores lógicos o vSockets) será igual al número de procesadores físicos (sockets) multiplicado por el número de cores del procesador. En un entorno virtualizado, la capa de

* En VMware, a los host se les denomina host ESXi y al hipervisor VMkernel.

virtualización de crea un espacio contiguo de memoria accesible para la máquina virtual cuando esta se inicia. El espacio de memoria asignado se configura durante la creación de la máquina virtual y tiene las mismas propiedades que el espacio de direcciones virtuales. Con esta configuración, el hipervisor puede ejecutar varias máquinas virtuales a la vez, impidiendo al mismo tiempo que las máquinas virtuales accedan a otra memoria que no sea la propia.

La virtualización de una red es la reproducción completa en software de una red física. Los componentes de redes fundamentales en la arquitectura virtual son los adaptadores Ethernet virtuales y los switches virtuales. La tecnología de VMware permite conectar máquinas virtuales locales entre sí y con la red externa por medio de un switch virtual. Los switches virtuales permiten que las máquinas virtuales de un mismo host ESXi se comuniquen entre sí con los mismos protocolos que utilizan los switches físicos, pero sin necesidad de utilizar hardware adicional. El switch Ethernet puede conectar varias vmnics (tarjetas de interfaz de red físicas) de forma que las máquinas virtuales que hacen uso del switch virtual tienen mayor disponibilidad y ancho de banda. Los switches virtuales permiten la segmentación de VLAN a nivel de puerto, por lo que cada puerto se puede configurar como puerto de acceso o puerto trunk y ofrecer acceso a una o a varias VLAN.

Los switches virtuales, al igual que los físicos, permiten aislamiento. Sin embargo, no requieren de un protocolo de árbol de expansión, ya que se impone una topología de red de un solo nivel. Los distintos switches virtuales no pueden conectarse entre sí; el tráfico de red no puede pasar directamente de un switch virtual a otro del mismo host. Los switches virtuales proporcionan todos los puertos que se necesitan en un solo switch.

El sistema de archivos de una arquitectura virtual permite acceso de lectura y escritura a un archivo determinado al mismo tiempo, usando un registro distribuido para los cambios en los metadatos y permitiendo una recuperación rápida y fiable en caso de fallo hardware. Es compatible con los diversos protocolos de almacenamiento: Fiber Channel, Fiber Channel sobre Ethernet, iSCSI y NAS. Permite además el crecimiento dinámico del contenedor del almacenamiento de datos [1].

2.3. Ventajas de la virtualización

Las principales ventajas de la virtualización son expuestas a continuación [1] y [2]:

Aislamiento: las máquinas virtuales son totalmente independientes, entre sí y con el hipervisor. Por tanto, un fallo en una aplicación o en una máquina virtual afectará únicamente a esa máquina virtual, el resto de máquinas virtuales y el hipervisor seguirán funcionando normalmente. Este aislamiento evita los conflictos de dependencia del software.

Seguridad: cada máquina tiene un acceso privilegiado (root o administrador) independiente. Por tanto, un ataque de seguridad en una máquina virtual sólo afectará a esa máquina. Esto permite aislar los servicios más críticos configurándolos en máquinas virtuales independientes.

Flexibilidad: podemos crear las máquinas virtuales con las características de CPU, memoria, disco y red que necesitemos, sin necesidad de "comprar" un servidor físico con esas características. También podemos tener máquinas virtuales con distintos sistemas operativos, ejecutándose dentro de una misma máquina física.

Agilidad: la creación de una máquina virtual es un proceso muy rápido, básicamente la ejecución de un comando. Por tanto, si necesitamos un nuevo servidor lo podremos tener casi al instante, sin pasar por el proceso de compra, configuración, etc. Acelerando y simplificando el aprovisionamiento de recursos y aplicaciones

Escalables. La virtualización permite ampliar la capacidad de un servidor virtual en cualquier momento y pasar a utilizar más recursos. De esta forma, podemos adaptar las prestaciones de un servidor en función de las necesidades del servicio en cada momento.

Compatibilidad ante cambios hardware: La virtualización permite introducir cambios en el hardware sin introducir cambios en los servidores virtuales, al ser este software en su totalidad. Esto nos permite mantener las aplicaciones y sistemas operativos heredados en un nuevo hardware cuando venzan los contratos de mantenimiento de los servidores físicos o se cambien estos.

Portabilidad y encapsulamiento: toda la configuración y el estado completo de una máquina virtual reside en uno o varios ficheros. Esto hace que sea muy fácil clonar o mover la máquina virtual a otro servidor físico, simplemente copiando y moviendo dichos ficheros que encapsulan la máquina virtual.

Recuperación rápida en caso de fallo y el tiempo para la copia de seguridad: si se dispone de una copia de los ficheros de configuración de la máquina virtual, en caso de desastre la recuperación será muy rápida, simplemente arrancar la máquina virtual con los ficheros de configuración guardados. No es necesario reinstalar, recuperar backups y otros procedimientos largos que se aplican en las máquinas físicas. Además, permite aprovisionar o migrar cualquier máquina virtual a cualquier servidor físico, permitiendo que, si un servidor físico tiene fallos, la máquina virtual que se ejecuta en él pueda ser migrada a otro servidor físico con funcionamiento óptimo con pérdida de servicio mínima.

Consolidación de servidores: Consiste simplemente en la reducción del número total de servidores. Con la optimización en la utilización de los recursos físicos de los servidores, mediante la virtualización, necesitaremos muchos menos recursos físicos y esto posibilitará la consolidación de servidores y recursos.

Administración: Se dispone de una única consola de administración que permite controlar más fácilmente los servidores virtuales y los servidores físicos que los alojan. Permitiendo de este modo una administración centralizada y homogénea.

Continuidad de negocio: La virtualización permite desarrollar de forma más eficiente políticas de continuidad del negocio con soluciones de recuperación ante desastres mejoradas y proporcionar alta disponibilidad y redundancia en todo el centro de datos.

Balanceo y disponibilidad de carga: Los servidores estarán preparados para responder a cambios en las cargas de trabajo.

Entornos de desarrollo: La virtualización nos permite probar las configuraciones de un software de manera más sencilla, simulando ambientes de trabajo para desarrollo/pruebas sin poner en riesgo los sistemas en producción. Además, los sistemas de prueba se pueden poner en producción fácil y rápidamente.

Por último, la virtualización permite ejecutar aplicaciones multiplataforma de una manera más sencilla y eficiente, permite disponer de sistemas completos probados por fabricantes y una máxima explotación de los recursos de hardware

Con todas estas ventajas, era conveniente realizar también un estudio pormenorizado de las desventajas de la virtualización. Las principales desventajas que consideramos son:

Menor rendimiento, dado que una máquina virtual corre en una capa intermedia a la del hardware real, siempre tendrá un rendimiento inferior. La degradación dependerá de la tecnología de virtualización utilizada, de la configuración realizada a nivel hipervisor y de la propia aplicación. Por regla general, las aplicaciones que más repercuten la pérdida de rendimiento son las que realizan operaciones frecuentes de entrada/salida. Sin embargo, esta penalización en el rendimiento cada vez es mucho menor debido a las mejoras en las versiones del software de virtualización y su cada vez mayor compatibilidad y adaptación a los servidores físicos al fabricarse estos cada vez más orientados a la virtualización.

Soporte y manejo de la nueva tecnología: El aspecto del soporte puede ser, en los inicios e introducción a la virtualización, una de las mayores preocupaciones. Sin embargo, los cursos formativos sobre la administración de los sistemas virtualizados, el soporte que incluyen los principales fabricantes de herramientas de virtualización y las comunidades de usuarios, permiten que esta desventaja se convierta hoy en día en insignificante.

Portabilidad: La portabilidad entre plataformas está condicionada a la solución de virtualización adoptada.

2.4. VMware frente a otras tecnologías de virtualización

Entre los principales proveedores de software que han desarrollado tecnologías de virtualización integrales (que abarcan todas las instancias: servidor, aplicaciones, escritorio) se encuentran, ordenados por cuota de mercado: VMware, Microsoft y Citrix. Estas compañías han diseñado soluciones específicas para virtualización, como son respectivamente VMware ESX, Hyper-V y XenServer para la virtualización de servidores. Las soluciones de virtualización que ofrecen cualquiera de estas 3 compañías proporcionan grandes prestaciones. La comparativa exhaustiva entre las tres tecnologías punteras de virtualización puede analizarse en [3][4]. VMware ofrece incluso

herramientas en forma de calculadora* que permiten calcular/demostrar cómo, para unas mismas prestaciones a conseguir en la arquitectura virtual, la solución de VMware exige una menor inversión en la infraestructura virtual que con Hyper-V y XenServer. Además, ofrece información del coste aproximado de cada partida de costes.

De estas tecnologías de virtualización punteras, se eligió VMware porque es el fabricante con la tecnología de virtualización más madura, potente y puntera del mercado. Además, dispone de un servicio de soporte excelente, compatibilidad con todos los fabricantes, gran oferta de cursos formativos y la mejor comunidad de usuarios. Su inconveniente puede ser un precio mayor en el coste de las licencias pero dispone de gran variedad de ofertas que ayudan a elegir una solución que se adapte a las necesidades de la empresa. Por otro parte, VMware es el líder del mercado de la virtualización y el que ofrece una compatibilidad más amplia y mejores actualizaciones de sus productos. Las soluciones de computación en la nube (cloud computing) que ofrece VMware pueden verse en la siguiente figura [5]:

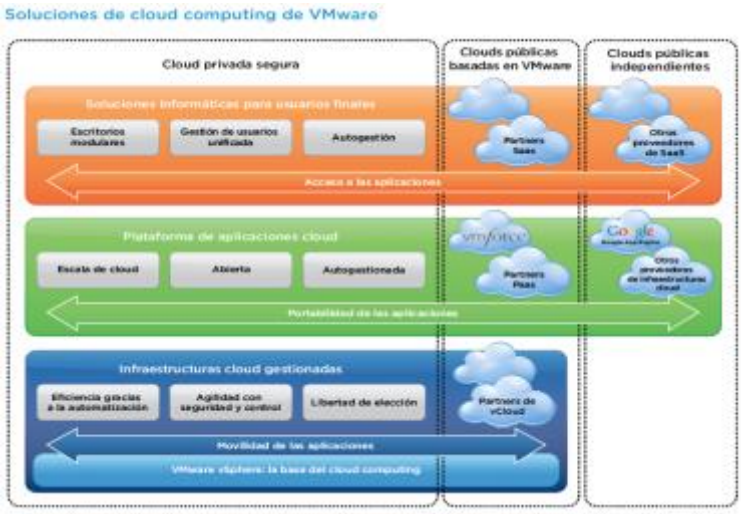


Figura 3: Soluciones de computación en la nube de VMware (tomada de [1])

De las soluciones de computación en la nube anteriores la que mejor se adaptada a los servicios que nuestra empresa quería proporcionar era la infraestructura de nubes gestionadas. Esta solución está basada en VMware vSphere 5.0 [6], que es la solución de virtualización que permite una administración y gestión centralizada de la plataforma virtual. VMware vSphere 5.0 engloba los productos:

* Dicha calculadora puede encontrarse en el siguiente enlace: http://www.VMware.com/go/tcocalculator/index.html

- VMware hipervisor ESXi: que introduce una capa de virtualización sólida y de alto rendimiento que separa los recursos de hardware del servidor y permite que varias máquinas virtuales los compartan.
- VMware Vcenter Server: proporciona una gestión unificada de la plataforma virtual creada con VMware vSphere a fin de automatizar y proporcionar una infraestructura virtual con total confianza. Se necesita una instancia de vCenter Server para gestionar de manera centralizada las máquinas virtuales y sus hosts, así como para habilitar todas las características de VMware vSphere.

Además, VMware vSphere incluye otras características indispensables: sistema de ficheros VMFS que permite almacenamiento compartido; alta disponibilidad; migración de máquinas entre hosts físicos (vMotion); planificador de distribución de recursos (DRS); o protección de las máquinas virtuales con cero indisponibilidad (*Fault tolerance*). Todas estas herramientas y características serán analizadas con profundidad en los capítulos posteriores.
Las otras soluciones de computación en la nube que ofrece VMware permiten crear servicios en la nube. La funcionalidad de nube de VMware permite al personal informático dar acceso a los usuarios a los centros de datos virtuales mediante un portal web, así como crear un catálogo de servicios de TI e implementarlos en el propio centro de datos virtual. No optamos por este tipo de soluciones porque nuestra empresa no iba a ofrecer servicios de cómputo en la nube a través de la infraestructura virtual ni a los clientes internos (departamentos) ni a los clientes externos (colectivo profesional). El objetivo perseguido con la implantación de la arquitectura virtual era utilizar todas las ventajas que ofrece la virtualización y ofrecer servicios y aplicaciones del mismo modo que lo hacíamos con la plataforma de servidores. Los recursos que ofrece la plataforma virtual no serán ofertados para su uso y gestión, sino que estos serán gestionados exclusivamente por el departamento tecnológico, que será el encargado de diseñar e implantar las aplicaciones que darán servicio a los clientes, sin que estos tengan posibilidad de gestionar recursos de la plataforma virtual.

Otras opciones valoradas fueron la de utilizar soluciones que consistían en el alojamiento de los servidores virtuales en nubes públicas en compañías como Amazon o Microsoft. El comité directivo de la empresa era muy reacio a almacenar determinados datos sensibles del colectivo profesional en grandes multinacionales donde estaría en entredicho el cumplimiento de la LOPD española o donde se desconocía dónde se realizaba realmente el almacenamiento físico de los datos. Por este motivo se decidió optar por una virtualización a nivel privado y, en el futuro, se podrían valorar la inclusión

escalonada de servicios menos críticos, en cuanto al nivel de protección de los datos utilizados, en cloud públicas.

2.5. Resumen y conclusiones

En este capítulo se ha tratado de describir la situación de la empresa al inicio del proyecto y todas las motivaciones, tecnológicas y no tecnológicas, que influyeron en la implantación de la arquitectura virtual. Se ha descrito las partes más importantes que componen una infraestructura virtual y las numerosas ventajas que supone la introducción de la virtualización en un parque de servidores con respecto a la arquitectura física. Por último, se ha justificado la elección de VMware como tecnología de virtualización dentro de las opciones de mercado existente centrándose en su solución VMware vSphere.

Capítulo 3:

3. Análisis y diseño global de la arquitectura virtualización

En este capítulo se van a describir detalladamente las tareas de diseño llevadas a cabo para la definición de los elementos que componen la arquitectura virtual basada en tecnología VMware. Cabe resaltar que desplegar una infraestructura virtual mediante VMware es mucho más que virtualizar servidores ya que existen otros elementos de vital importancia como el almacenamiento, las redes o la seguridad.

3.1. Análisis y Planificación

Para que cualquier proyecto de virtualización se realice con éxito y proporcione el mejor retorno de la inversión posible, es esencial una amplia planificación previa a la migración. Por ello, es preciso llevar a cabo una investigación exhaustiva antes de iniciar el proyecto.

La primera tarea a realizar es analizar la infraestructura de la que se parte e identificar los posibles candidatos para la consolidación de servidores[*], es decir, identificar aquellos servidores físicos de los cuáles se va a prescindir, ya que no eran aprovechables para formar parte de la arquitectura virtual o complementar esta. Los servicios de estos servidores físicos se van a migrar a la infraestructura virtual completándose la consolidación. Los activos hardware que componían el parque de servidores antes del proceso de virtualización son expuestos a continuación:

- Arquitectura con hardware y software del fabricante Apple, totalmente independiente del resto de servidores, ya que, como la mayoría de productos Apple, contaba con un modo de funcionamiento y administración totalmente exclusiva de este fabricante y no podía integrarse con productos de otros fabricantes. La arquitectura estaba compuesta por 6 servidores *Xserves* y dos cabinas de almacenamiento *XRAID* que utilizaban una red SAN Fiber Channel formada por 2 switches *FC SANBOX*. La venta de productos de Apple en el mercado de servidores fue

[*] es un proceso de reducción del número total de servidores físicos, con el consiguiente ahorro económico al reducirse el mantenimiento de los servicios y las averías y conseguir un mejor aprovechamiento de los recursos.

discontinuada en noviembre de 2010 y con ella también se discontinuó el soporte a sus productos en el mercado. Tampoco ofrecían soporte a actualizaciones a nivel de sistema operativo para corregir bugs de funcionamiento y parches de seguridad. Por ello, contábamos con una arquitectura de servidores Apple sin continuidad en hardware y software ni soporte del fabricante. Por este motivo, esta arquitectura debía ir desmantelándose, finalizando su ciclo de vida, y sus servicios deberían ser migrados a la arquitectura virtual.

- Dos servidores HP bajo sistema operativo Linux Red Hat que iban a ser dados de baja por su antigüedad. Estos dos servidores fueron adquiridos en 2004 y contaban con 9 años de servicio. Se utilizaban como hospedaje web y los mínimos servicios prestados en este tiempo serían migrados a máquinas virtuales de la arquitectura virtualizada a implantar.
- Tres servidores DELL con sistema operativo Windows Server 2003 que fueron adquiridos en 2008 y daban servicios importantes internos en mi empresa de Active Directory, servicios de gestión del programa contable para el departamento de contabilidad, y servidor de seguridad/Antivirus. Estos servidores no se iban a migrar de momento a la infraestructura virtual ya que se decidió dejarlos fuera de este proceso inicial de consolidación. Se consideraría su migración en un futuro más a largo plazo sobre todo porque albergaban aplicaciones críticas en el funcionamiento de la empresa y porque podían seguir prestando el servicio para el que fueron adquiridos sin ningún problema. Una vez estuviera funcionando la arquitectura virtual de forma óptima se consideraría su migración al entorno virtual.
- Dos cabinas de almacenamiento modelo Promise Vtrak que funcionaban bajo sistema de almacenamiento NAS para dar servicio de ficheros interno a la empresa.
- Dos servidores DELL OEM Power Edge R410 que llevaban un año dando servicio bajo sistema operativo Linux Ubuntu.

De los servidores descritos anteriormente, no se podían considerar para la virtualización a los servidores de Apple, porque aparte de estar sin continuidad en hardware y soporte, estos servidores no permiten ningún tipo virtualización. Tampoco se iban a incluir los dos servidores HP que tenían más de 9 años de antigüedad ya que disponían de unas características hardware muy pobres, eran modelos discontinuados y sin soporte, y su configuración hardware ni permitía ni cumplía los requisitos mínimos para la virtualización con VMware vSphere. Del mismo modo, como ya se razonó anteriormente tampoco se incluirían los 3 servidores DELL con sistema operativo Windows Server 2003. En cuanto a las cabinas de almacenamiento, dejarían de dar servicios de producción y se utilizarían únicamente para copias de seguridad. Tras descartar por diversas razones el resto de

servidores, se llevaría a cabo la consolidación manteniendo en el parque de servidores físicos los dos servidores DELL OEM Power Edge R410, que serían virtualizados para utilizarlos en la infraestructura virtual.

Existen diversos productos que pueden ayudar a que el proceso de identificar candidatos a la virtualización sea un proceso significativamente más directo. El producto más destacado y utilizado en el mercado es **VMware Capacity Planner** [7]: es la herramienta de VMware para la estimación y el análisis de las necesidades de equipamiento para grandes proyectos de virtualización, denominada habitualmente consolidación. Es una herramienta que proporciona ayuda para dimensionar la infraestructura de hardware que vamos a necesitar para consolidar nuestros servidores físicos en ESXi. Es un servicio en la nube* al que reportan colectores de datos instalados en la red a consolidar, por tanto, no hay que mantener ninguna infraestructura para disponer de este.

Este tipo de herramientas tan potentes se utilizan en grandes proyectos de consolidación de más de decenas servidores. Por ello, aunque analizamos y consideramos de forma inicial este tipo de herramientas para la planificación de qué servidores se debían virtualizar o cuántos servidores físicos comprar, al final realizamos un cálculo mucho más manual que se ajustaba a nuestra situación y necesidades específicas.

3.2. Identificación Licencias VMware

Durante el diseño de la arquitectura virtual de mi empresa, la versión más actual de VMware vSphere era la versión 5. Las licencias de VMware vSphere 5 se conceden por cada procesador físico, de cada host ESXi presente en la arquitectura virtual, con asignación de derechos de memoria virtual agrupada en pool (vRAM) [8]. Cada licencia de procesador físico de VMware vSphere 5 incluye derechos para una capacidad determinada de vRAM, es decir, de memoria configurada para las máquinas virtuales. Según lo anterior, para la arquitectura virtual a desplegar se necesitarán una licencia de VMware vSphere 5 para cada CPU de cada ESXi. Además, como se analizará con detalle más adelante en la sección 4.2, en la arquitectura virtual dispondremos de una instancia de VMware vCenter, que es un componente que proporciona la gestión unificada del entorno VMware vSphere y para el cual se necesita una licencia específica.

* Disponible en http://optimize.VMware.com

Las licencias de VMware vSphere 5 están agrupadas en un pool, es decir, se agregan, para todas las licencias de CPU gestionadas por una instancia de VMware vCenter (o varias instancias de VMware vCenter enlazadas) para constituir la capacidad total de vRAM disponible *(capacidad del pool de vRAM).* No existen restricciones respecto a cómo se configura la vRAM en las máquinas virtuales y las CPU. En cualquier momento la cantidad de vRAM configurada por las máquinas virtuales encendidas en una CPU podría superar los derechos base correspondientes a la licencia de vSphere 5 asignada a esa CPU. No existen restricciones respecto al número de máquinas virtuales que se pueden ejecutar en un pool, siempre y cuando la vRAM total configurada en todas las máquinas virtuales gestionadas por una instancia de VMware vCenter sea menor o igual que la vRAM total disponible. Siempre que se cumpla la condición anterior, las licencias de vSphere son correctas.

Para mantener la conformidad de las licencias, en todo momento se deben cumplir las condiciones siguientes:

- Cada procesador físico (CPU) activo debe tener asignada al menos una licencia.
- El promedio acumulado de 365 días del límite diario de la vRAM configurada para todas las máquinas virtuales encendidas sumadas no puede superar la capacidad del pool de vRAM.
- Las licencias de vSphere deben ser adquiridas antes de usarlas. La manera más sencilla de expandir la capacidad del pool de vRAM es agregarle más licencias de CPU de VMware vSphere, pero siempre de la misma edición. También podemos aumentar el pool de vRAM actualizando todas las licencias de CPU del pool de vRAM a una edición de VMware vSphere con más derechos de vRAM. Otra opción puede ser añadiendo otro host con nuevas licencias de la misma edición de vSphere que el pool existente.

En cuanto al vCenter Server, está disponible en los siguientes paquetes:

- VMware vCenter Server *Essentials Kits*: gestión integrada para los kits de VMware vSphere *Essentials*.
- VMware vCenter Server Standard: gestión muy escalable que agiliza la administración y gestión de las máquinas virtuales de un entorno VMware vSphere así como la aplicación sobre la infraestructura virtual de las funcionalidades avanzadas de VMware vSphere. Se utiliza en los Kits *Standard, Enterprise y Enterprise Plus*. Permite gestionar hasta un máximo de 1000 ESXi y 10000 máquinas virtuales.

- VMware vCenter Server Foundation: gestión centralizada de un máximo de tres host de VMware vSphere. Sería como la versión Standard anterior pero solo hasta 3 ESXi.

VMware ofrece varias opciones de paquetes diseñados para una amplia variedad de situaciones de implementación. Las ediciones de VMware vSphere ofrecen varias combinaciones de funcionalidad y derechos de vRAM con distintos precios proporcionando una vía para satisfacer los requisitos concretos de escalabilidad, tamaño del entorno y casos de uso. Además, VMware ofrece los denominados kits, que son soluciones que incluyen varias licencias de VMware vSphere y vCenter Server en conjunto con mayores ventajas económicas. En la siguiente figura se muestran los tipos de licencias y kits disponibles de VMware Vsphere:

	Standard	Enterprise	Enterprise Plus
Derechos por licencia de CPU • Derechos de vRAM • vCPU/MV	32 GB 8 vías	64 GB 8 vías	96 GB 32 vías
Funciones • Hypervisor	✓	✓	✓
• High Availability • Data Recovery • vMotion	✓ ✓ ✓	✓ ✓ ✓	✓ ✓ ✓
• Virtual Serial Port Concentrator • Hot Add • vShield Zones • Fault Tolerance		✓ ✓ ✓ ✓	✓ ✓ ✓ ✓
• Storage APIs for Array Integration • Storage vMotion • Distributed Resource Scheduler y Distributed Power Management		✓ ✓ ✓	✓ ✓ ✓
• Distributed Switch • Network I/O Control y Storage I/O Control • Host Profiles			✓ ✓ ✓
• **Auto Deploy*** • **Policy-Driven Storage*** • **Storage DRS***			✓ ✓ ✓
*Nuevo en vSphere 5.0			

	Essentials	Essentials Plus	Standard AK	Enterprise AK	Enterprise Plus AK
Incluye	6 CPU	6 CPU	8 CPU	6 CPU	6 CPU
Derechos por licencia de CPU • Derechos de vRAM	32 GB (192 GB máx.)	32 GB (192 GB máx.)	32 GB (256 GB máx.)	64 GB (384 GB máx.)	96 GB (576 GB máx.)
• vCPU	8 vías	8 vías	8 vías	8 vías	32 vías
Funciones • Hypervisor	✓	✓	✓	✓	✓
• High Availability • Data Recovery • vMotion		✓ ✓ ✓	✓ ✓ ✓	✓ ✓ ✓	✓ ✓ ✓
• Virtual Serial Port Concentrator • Hot Add • vShield Zones • Fault Tolerance				✓ ✓ ✓ ✓	✓ ✓ ✓ ✓
• Storage APIs for Array Integration • Storage vMotion • Distributed Resource Scheduler y Distributed Power Management				✓ ✓ ✓	✓ ✓ ✓
• Distributed Switch • Network I/O Control y Storage I/O Control • Host Profiles					✓ ✓ ✓
• **Auto Deploy*** • **Policy-Driven Storage*** • **Storage DRS***					✓ ✓ ✓
*Nuevo en vSphere 5.0					

Figura 4: Ediciones y kits de VMware vSphere 5.0 (tomada de [7]).

En la tabla de la izquierda se muestran los tipos de licencia por CPU física que ofrece VMware y las funcionalidades incluidas en cada una de ellas. También puede verse los derechos de vRAM y el número máximo de CPU virtuales que puede asignarse a cada máquina virtual a desplegar al utilizar cada tipo de licencia.

En la tabla de la derecha pueden visualizarse los kits de licencias que ofrece VMware y las funcionalidades incluidas en cada uno de ellos. Para cada tipo de kits se muestra el número de licencias por CPU que incluye, los derechos de vRAM asociados y el número máximo de CPU

virtuales que puede asignarse a cada máquina virtual a desplegar al utilizar cada tipo de kits. En cada kits se incluye una licencia de Vcenter Server del tipo referenciado en el kit.

Una vez conocido de forma exhaustiva la forma de licenciar y los tipos y kits de licencias disponibles, seleccionamos para nuestra arquitectura virtual aquella que mejor se adaptaba a nuestras necesidades teniendo en cuenta la relación prestaciones/precio que podíamos adquirir. Según esto, la versión instalada de VMkernel para los seis servidores ESXi que se eligió fue VMware ESXi 5 Update 1 con licencia Standard.

Como se detalla en el siguiente apartado de este capítulo, el número de CPUs físicas disponible en nuestro clúster de ESXi era de 12 procesadores, 2 por cada host ESXi, por lo que el número de licencias a adquirir era también de 12. Además, dispondremos de una instancia de VMware Vcenter Server. Con el fin de buscar la manera más económica para la adquisición de las licencias VMware Vsphere 5 Standard contratamos lo siguiente:

- 1 Standard Acceleration kit para 8 procesadores (con 32 GB vRAM por cada procesador(256GB máx) y 8 vCPU/MV).
- 4 licencias VMware vSphere 5 Standard para 1 procesador (con 32 GB VRAM por cada procesador y 8 vCPU/MV).

Por último, resaltar que cada licencia o kit de VMware vSphere requiere un contrato de soporte y suscripción (SnS) de un año y este soporte debe ser renovado anualmente.

3.3. Diseño pool de recursos arquitectura virtual

En este apartado se va describir de forma detallada el proceso de diseño del pool de recursos que queremos tener disponible en la arquitectura virtual.

3.3.1. Diseño de CPU en infraestructura de VMware vSphere

En el diseño de una infraestructura virtual, el dimensionamiento de la CPU no es uno de los parámetros más críticos ya que lo normal es que las limitaciones o cuellos de botella de la

arquitectura no se produzcan por falta de este recurso. Suele ser un parámetro que viene muy bien dimensionado en los servidores físicos y dispondremos de capacidad de sobra. Sin embargo, es importante considerar este parámetro de diseño porque influye en otros parámetros que sí son mucho más críticos.

En primer lugar, analizaremos los diferentes conceptos para diseñar los recursos de procesamiento en una infraestructura de vSphere. Comenzaremos con una comparativa entre un modelo "Scale Up" y uno "Scale Out" con sus pros y contras correspondientes. Veremos además otros ítems importantes que ayudarán a tomar las decisiones correctas.

Lo primero que debemos tener claro en un proceso de diseño que parte de cero es si trabajaremos en modo "Scale Up" o "Scale Out". Un modelo "Scale Up" está compuesto por un número reducido de Hosts físicos con grandes recursos de CPU, permitiendo de esta forma dar servicio a un número importante de Máquinas Virtuales en menos Hosts. Por otra parte, un modelo "Scale Out" se compone de un mayor número de Hosts físicos con unas prestaciones más bien estándar. De esta forma las Máquinas Virtuales estarán repartidas entre un número mayor de Hosts:

	Scale Up	Sale Out
Número de Host	Menor	Mayor
Coste por Host	Elevado	Normal
Licenciamiento*	Menor nº CPU	Mayor nº CPU
Mantenimiento**	Menor	Mayor
Ratio VM/Host	Muy alto	Normal
Espacio en CPD	Menor	Mayor
Consumo en CPD***	Menor	Mayor
Tiempo de recuperación y HA****	Mayor	Menor
Orientado a *****	Más MVs	Menos MVs

** Normalmente el número total de CPUs es menor en un modelo Scale Up.*
***Tiempos de despliegue, actualización, migración, mantenimientos y gestión.*
****El coste de enfriamiento y alimentación es menor en un modelo Scale Up.*
*****Los tiempos de recuperación en una caída afectan en mayor medida a un modelo Scale Up*
******Un modelo Scale Up está orientado para un número importante de Máquinas Virtuales*

Tabla 1: Modo Scale up y Scale Out

Como se puede observar en la tabla anterior, el modelo "Scale Up" exige un mayor desembolso económico por host, ya que estos tienen muchas más prestaciones. Sin embargo, este modelo proporciona mejores prestaciones en el mantenimiento y tiempos de recuperación, y compensa el mayor desembolso inicial al necesitar menos espacio y consumo en el CPD y menor número de licencias al disponer de menor número de host con mayores prestaciones. Por otro lado, el objetivo estimado era alojar en nuestra arquitectura virtual un número elevado de máquinas virtuales, **en torno a 30 – 40 máquinas virtuales**, según se fueran consolidando los nuevos proyectos, para un plazo estimado de **unos 4 años**. Por todas las razones anteriores, el modelo que mejor se adaptaba a nuestras necesidades era el modelo "Scale Up".

Un ítem importante en nuestro diseño era determinar el número de vCPUs que aprovisionaremos por cada core físico que dispongamos. Una buena práctica recomendada [9] por VMware es aplicar un ratio de **entre 4 - 8 vCPUs por cada core físico**. Este parámetro va a depender

en gran medida del tipo de aplicaciones a desplegar. En nuestro caso seguimos una política conservadora en este sentido puesto que la mayoría de las aplicaciones que vamos a alojar en la infraestructura virtual a desplegar están por desarrollar y, por este motivo, no conocemos los recursos óptimos reales que necesitarán. De este modo, una vez desplegada la arquitectura virtual y en la fase de *test* de las aplicaciones podremos realizar las medidas adecuadas de necesidades de procesamiento de las mismas y ajustar las necesidades de los servidores virtuales en los que se alojarán. Por este motivo, vamos a fijar el ratio de vCPUs por cada core físico en un valor de 4 para el diseño. Para conseguir que existan más CPU virtuales que físicas VMware utiliza un módulo software denominado multiprocesador simétrico virtual (vSMP) que permite a las máquinas virtuales tener acceso a más de una CPU física que se asignarán como CPU virtuales.
Otro dato a resaltar es que el número de vCPUs a asignar a las máquinas virtuales a crear está limitado por el tipo de licencia de VMware vSphere que se contrate: Standard a 8 vCPUs, Enterprise a 16 vCPU, y Enterprise Plus a 64 vCPUs (puede visualizarse con detalle en la figura 4).

Para disponer de alta disponibilidad en nuestro entorno debemos contar con recursos suficientes. Para ello, debemos definir el número de hosts caídos de forma simultánea que la infraestructura virtual a desplegar deberá asumir y de ese número saldrá la reserva que deberemos aprovisionar para cumplir con los recursos necesarios de alta disponibilidad. Del mismo modo, fijaremos una tasa de crecimiento estimada que nos servirá de garantizar el crecimiento del clúster a corto plazo y, en las fases iniciales, para posibles desviaciones en las estimaciones o albergar posibles recursos no previstos. Los recursos necesarios para cubrir la tasa de crecimiento estimada se pueden ir aprovisionando según se vayan necesitando más recursos. El objetivo es soportar la caída de un host dentro del clúster y contar con una estimación de crecimiento del 20% en los próximos cuatro años.

Para analizar el aprovisionamiento de CPU y el número máximo de máquinas virtuales que podremos desplegar en nuestra arquitectura virtual a implementar realizamos los siguientes cálculos[*]:

- Número máximo máquinas virtuales estimadas a desplegar: **40 máquinas virtuales**.
- Número de vCPUs por Máquina Virtual: Estimaremos una media de 3 vCPUs por máquina virtual.
- Número de vCPU a aprovisionar: 3 vCPUs/MV * 40 MV = **120 vCPUs**.
- Ratio de consolidación vCPU/Core a utilizar es de **4 vCPUs**.

[*] Puede consultarse una calculadora similar a los cálculos seguidos en el proceso de diseño en *Server Virtualization Calculator* http://wintelguy.com/vmcalc.pl

- Número total de cores físico necesario: 120 vCPU entre 4vCPUs/core = **30 cores.**
- Capacidad adicional para crecimiento estimado: 20%. El 20% de 30 cores son 6 cores adicionales para garantizar el crecimiento sobre el clúster a corto plazo. Según esto, necesitaríamos **36 cores**.
- Características de los procesadores físicos a utilizar en los hosts: van a determinar el número de servidores físicos necesarios en la arquitectura virtual para provisionar los 36 cores necesarios. Los 2 servidores DELL ya adquiridos y en funcionamiento en la empresa, que se iban a utilizar dentro del clúster de host de la arquitectura virtual, disponían de 2 procesadores físicos cada uno (sockets) de 4 cores. Teniendo en cuenta estos dos servidores, nos quedarían por aprovisionar: 36 – 16 = 20 cores, para los cuales podríamos utilizar uno o dos servidores de características muy superiores a los que ya disponíamos o tres servidores de características muy similares a los ya adquiridos. Con el fin de disponer de un clúster de elementos muy similares que nos permitan cumplir con las condiciones de alta disponibilidad que necesitábamos, en caso de caída de un host, y con un pool de recursos aportado de forma uniforme por todos sus hosts físicos, adquirimos servidores con características idénticas a los que ya disponíamos: 2 procesadores físicos de 4 cores. Esta distribución uniforme en el aporte de recursos en los servidores físicos dentro del clúster nos permitía que todos los nodos del clúster fuera idénticos en importancia y ante algún fallo en alguno de ellos no provocara ninguna descompensación a la hora de asumir los recursos necesarios para levantar las máquinas virtuales que estuviera asumiendo el host caído. Además, el hecho de utilizar CPUs similares o idénticas permite que funcionen de forma más óptima características propias de la arquitectura física del servidor como por ejemplo NUMA*. Según lo anterior para provisionar los 20 cores restantes necesitamos adquirir 3 servidores nuevos: 20 cores entre 8 cores/servidores = **3 servidores**.
- Capacidad extra para alta disponibilidad: Al considerar que nuestra arquitectura debe soportar la caída de un host, debemos adquirir otro nuevo host adicional con 2 Sockets de 4 cores físicos.

En resumen, como hemos visto anteriormente el clúster físico de la arquitectura virtual estará compuesto por 6 host ESXi con 2 procesadores físicos de 4 cores cada uno: 6 x (2x4) = **48 cores físicos**. El objetivo es soportar la caída de un host dentro del clúster (8 cores) y seguir funcionando sin ningún problema y, además, contar con una estimación de crecimiento del 20% en los próximos

* NUMA: cada procesador tiene acceso directo mediante un bus privado a unos bancos de memoria proporcionando acceso muchísimos más rápidos.

cuatro años (6 cores). Con estas reservas, el número de cores disponibles para asignar a las máquinas virtuales a crear sería de 34 cores. Como el ratio de consolidación vCPU/Core es de 4 a 1, obtenemos un total de 136 vCPUs disponibles para asignar a las máquinas virtuales a crear. El número de vCPUs por máquina virtual que consideraremos de media para hacer los cálculos del pool disponible será 3, obteniendo de este modo que nuestra arquitectura virtual funcionaría sin problemas con 40 máquinas virtuales. El estimar 40 máquinas virtuales a crear aproximadamente en los próximos 4 años permite a la infraestructura virtual asumir sin problemas a todos los servicios proporcionados en la actualidad y alojar a los servicios nuevos a implementar en los próximos años. Además, hay que tener en cuenta que hemos realizado una estimación bastante conservadora. El hecho de elegir 3 vCPUs como media en las máquinas virtuales es un valor de diseño aproximado teniendo en cuenta que trabajaremos con máquinas de producción que necesitarán más recursos y máquinas de desarrollo y preproducción donde podemos ajustar estos recursos de CPU. Hay que tener en cuenta que las mejores prácticas [8] de VMware recomiendan crear las máquinas virtuales con una única vCPU y solo aumentar este número en el caso de que las medidas de rendimiento posteriores así lo exijan. Una vez analizada la carga de la máquina virtual iremos añadiendo vCPU según la necesidad. Cuando la máquina virtual necesite realizar una operación, esta tendrá que esperar a que haya disponible una CPU física donde realizar la operación. Por este motivo, al añadir más vCPU se incrementa el riesgo de que el tiempo de espera de las CPU físicas aumente provocando un rendimiento peor. Si la carga de trabajo requiere múltiples vCPU, se deben configurar tan pocas como sea posible, con el fin de lograr unas mejores prestaciones a nivel de máquina virtual y a nivel de host.

Si bien en esta estimación no se han considerado la capacidad de proceso por CPU que necesitamos, la capacidad de procesamiento de la que se dispondrá y el número de vCPUs por cada máquina virtual debería cubrir con creces los requisitos de capacidad de proceso para todas las máquinas virtuales.

3.3.2. Clúster de Hosts ESXi en infraestructura VMware vSphere

Tal y como hemos visto en el apartado anterior, la arquitectura virtual estará formada por un clúster de 6 servidores físicos más un servidor independiente que se utilizará para tareas de administración, gestión y backups. Por lo tanto, un clúster de 6 Hosts ESXi se consideró una buena base para sustentar la implantación inicial de la infraestructura virtual teniendo en cuenta, además, que la arquitectura es fácilmente escalable y en cualquier momento se podrían añadir más recursos al

clúster. Del mismo modo, desde el punto de vista económico se estimó que era un buen número teniendo en cuenta las variables económicas hardware y software que entran en juego: prestaciones del propio servidor, licencias de virtualización VMware, costes de red Ethernet, costes de red de almacenamiento, housing del CPD, proveedor ISP, etc.). Teniendo en cuenta lo anterior se adquirieron 5 servidores para la plataforma virtual a desplegar (para unirse a los dos servidores DELL de los que ya se disponía):

- Dos servidores DELL OEM Power Edge R410, idénticos a los ya disponibles en nuestras instalaciones. Las características más importantes de estos servidores son expuestas a continuación [10]:
  - Doble procesador Intel Xeon E5506 (2.13GHz, 4C, 4M Cache, 800MHz/80W).
  - 24 GB RAM (6 x 4GB Dual Rank RDIMMS) a 1333MHz expansible a 288 GB.
  - 2 HDD 500GB SAS/SATA 7200 3,5".
  - Dos fuentes de alimentación redundadas.
  - 1 tarjetas de red Broadcom NetXtreme dual 1GbE NIC PCIe x4 con TOE.
  - 3 años de soporte Next Business Day on-site Service.

- Tres servidores IBM System x3550 M3. Las características más importantes de estos servidores son expuestas a continuación [11]:
  - doble procesador Intel Xeon E5506 (2.13GHz, 4C, 8M Cache, 1066MHz/80W).
  - 24 GB RAM (6 x 24GB Dual Rank RDIMMS) a 1333MHz expansible a 128 GB.
  - 2 HDD 300GB SAS/SATA 10000 2,5".
  - Fuentes de alimentación redundadas.
  - 1 tarjetas de red Intel Quad Port Server i340-T4
  - 3 años de soporte 24x7, 4 horas de respuesta.

Por lo tanto, nuestra arquitectura virtual estará sustentada por un clúster de 6 hosts ESXi, cuatro servidores DELL y dos IBM. Estos son los servidores físicos donde se ejecuta el kernel que proporciona VMware, que permite la virtualización de servidores virtuales. El servidor IBM restante albergará el VMware Vcenter Server y realizará tareas de administración y gestión adicionales que detallaremos en los capítulos siguientes.

Es importante resaltar que todos los servidores que formen parten de la arquitectura virtual deben ser completamente compatibles con VMware* para poder disponer de todo el soporte del fabricante ante cualquier incidencia.

3.3.3 Diseño de la memoria RAM en infraestructura VMware vSphere

En este apartado se van a analizar las consideraciones del diseño de la memoria RAM en la infraestructura a implantar. La cantidad de RAM suele ser el parámetro más crítico del pool de recursos en la infraestructura virtual, ya que determina en gran medida el número de máquinas virtuales que podremos desplegar en cada ESXi con funcionamiento óptimo. Sin embargo, es más crítica la gestión de este recurso que su diseño en sí. La máxima cantidad de memoria RAM posible de la que podremos disponer en la arquitectura virtual nos viene limitada por el licenciamiento VMware seleccionado: tipo de licencias y número de sockets. Para nuestro caso, con licenciamiento vSphere Standard, como ya calculamos en el capítulo anterior, el pool de vRAM sería:

Pool de VRAM disponible: 32 GB por CPU x 12 CPU = **384 GB**

La vRAM configurada, que es igual a la suma total de vRAM configurada en todas las máquinas virtuales encendidas gestionadas por nuestro VMware vCenter Server, siempre deberá ser menor que esta cantidad. Por lo tanto, en el clúster de host ESXi se pueden instalar como máximo 384 GB de memoria RAM, 64 GB de RAM por host para una distribución uniforme en los servidores del clúster.

Obviamente, la memoria RAM también nos vendrá limitada por la cantidad máxima de RAM que soporten los servidores que formarán el clúster de hosts. Como ya comentamos en el apartado anterior, nuestra arquitectura virtualizada seguirá un modelo "Scale up". Por este motivo, tendremos que diseñar una mayor cantidad de RAM por Host para conseguir los objetivos de máquinas virtuales marcados. Además, es interesante utilizar módulos de memoria de más capacidad con el objetivo de dejar libres bahías en los servidores para una más que segura ampliación de memoria en un futuro, lo que nos permitirá la escalabilidad de RAM de la plataforma sin la necesidad de adquirir nuevos servidores host físicos.

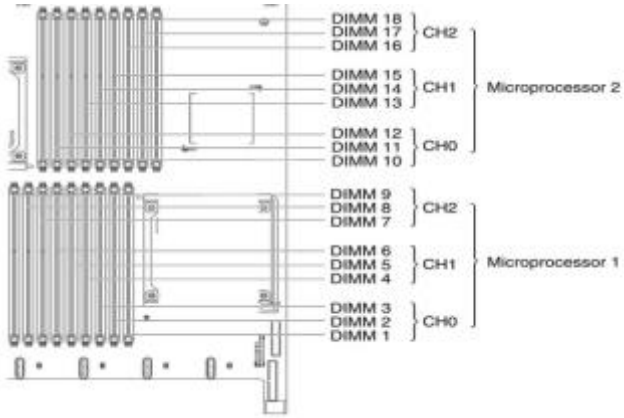
* Para comprobar si los servidores a adquirir son totalmente compatibles con VMware hay que consultar la Lista de Compatibilidad Hardware de VMware(HLC): http://www.VMware.com/resources/compatibility/search.php

Para nuestra infraestructura, como hemos comentado anteriormente, dispondremos de 6 servidores, los cuales disponen de forma inicial de 24 GB de RAM para cada ESXi. Por ello, dispondremos de un pool de memoria RAM física de 144 GB RAM. Esta memoria es ampliable en el futuro mediante la colocación de módulos de memoria en los servidores pues disponemos de bahías libres hasta el máximo que nos determina el tipo de licencia. Por este motivo, podremos adaptarnos fácilmente a las necesidades de memoria de nuestras máquinas virtuales cuando se consuma el pool de recursos de memoria RAM disponible de forma inicial. El tamaño máximo de memoria RAM que aceptan los servidores del clúster es de 128 GB en el caso de los servidores DELL y 288 GB en el caso de los servidores IBM. Concretamente en los modelos IBM x3550 M3 [11] podremos disponer de la siguiente distribución de memoria RAM DDR3 dependiendo del tamaño de los módulos elegido:

Numero de DIMMs	Tipo de DIMM	Tamaño de DIMM	Memoria total
12	Single-rank UDIMMs	2GB	24 GB
12	Dual-rank UDIMMs	4 GB	48 GB
18	Single-rank UDIMMs	2GB	36 GB
18	Dual-rank UDIMMs	2GB	36 GB
18	Dual-rank UDIMMs	4 GB	72 GB
18	Dual-rank UDIMMs	8 GB	144 GB
12	Quad-rank UDIMMs	16 GB	192 GB
18	Dual-rank UDIMMs	16 GB	288 GB

Tabla 2: Máxima cantidad de memoria RAM RDIMM a instalar

El tamaño de los módulos RDIMM soportados por el servidor son 2 GB, 4 GB, 8 GB y 16 GB. El servidor soporta un mínimo de 2 GB y un máximo de 288 GB usando el sistema de memoria RDIMMs (el registro permite que los RDIMM funcionen potencialmente a frecuencias más altas y admitan más DIMM dentro de un canal de memoria). La siguiente figura muestra la distribución de la memoria en la placa base del servidor por procesador y el orden de colocación óptima de los módulos de RAM:



Installed microprocessor	DIMM connector population sequence
Microprocessor socket 1	3, 6, 9, 2, 5, 8, 1, 4, 7
Microprocessor socket 2	12, 15, 18, 11, 14, 17, 10, 13, 16

Figura 5: Distribución y colocación óptima de los módulos de memoria (tomada de [27])

A la hora de colocar la memoria de forma inicial y para posibles ampliaciones futuras es importante seguir el orden que se indica en la figura anterior, y colocar el tamaño total que se va a insertar en la placa de forma simétrica, asignando el 50% de la misma a cada procesador. De este modo, conseguiremos un funcionamiento óptimo de los procesadores y su utilización de la memoria RAM. En el caso de los servidores del fabricante DELL que forman parte del clúster de nuestra arquitectura virtual el procedimiento está definido en [12].

3.4. Diseño de los servicios de red en infraestructura VMware VSphere

Una configuración de red adecuada es la piedra angular de una infraestructura viable VMware vSphere. Los servicios de red de vSphere definen una red virtual que proporciona funciones de red para hosts y máquinas virtuales. Los servicios de red permiten comunicación entre las máquinas virtuales y otras máquinas virtuales y físicas, y permiten la gestión del clúster de hosts ESXi.

La primera decisión importante a tomar es, sin duda, el diseño de los switches virtuales (vSwitch). Un vSwitch [1][2] es una estructura software implementada por el VMkernel que ofrece conectividad de red y gestión del tráfico para máquinas virtuales que se ejecutan en un host ESXi. Permite vincular

interfaces de red físicas y asignar conexiones, denominadas grupos de puertos, para crear redes de gestión y redes de datos entre máquinas virtuales. Existen 2 tipos de switches virtuales:

- **Switches estándar**: proporcionan configuración de switch virtual para un único host.
- **Switches distribuido**: proporcionan una configuración de switch virtual para un clúster de hosts ESXi, funcionando como un único switch virtual entre todos los hosts asociados. Disponen de múltiples funcionalidades adicionales.

Los switches distribuidos solo están disponibles para la licencia VMware vSphere 5 Enterprise Plus, con lo que a pesar de ser una funcionalidad muy potente, el coste de dicha licencia hacía imposible disponer de esta funcionalidad (cada licencia Enterprise Plus es aproximadamente 3 veces más cara que una Standard). Por ello, en nuestra arquitectura virtual, utilizaremos s*witches virtuales estándar*. Para disponer de una gestión de red similar a nivel de clúster, se replica la configuración de los switches virtuales estándar en todos los hosts que componen el clúster.

La siguiente cuestión a diseñar es el número de interfaces físicas de red que vamos a colocar en los hosts. Este número va a estar relacionado con el número de grupo de puertos que vamos a utilizar, la alta disponibilidad que queremos conseguir y la segmentación física que busquemos.

Para proporcionar la alta disponibilidad a la red gestión vamos a aprovisionar como mínimo dos interfaces de red físicas al grupo de puertos de gestión. Para obtener redundancia y alta disponibilidad debemos disponer de un mínimo de dos adaptadores de red físicos por cada host. Por lo tanto, cada host ESXi de nuestra arquitectura virtual va a disponer de 2 interfaces de red físicas activas para garantizar estas características fundamentales. Para garantizar la redundancia a nivel de tarjeta de red física en los host ESXi se ha combinado el uso tarjetas de red integradas en placa base con tarjetas de red de slots PCIe.

Para cada host ESXi físico, VMware vSphere permite colocar todas las redes en un único switch virtual estándar o en varios switches virtuales estándar, con una red independiente cada uno de ellos. La decisión depende de las redes físicas y del número de adaptadores de red disponibles. En nuestro caso, como no queremos tener una interfaz de red para cada switch virtual estándar, ya que exigiría disponer de un número muy elevado de interfaces de red físicas y añadiría complejidad a la gestión y a la redundancia, vamos a agrupar los adaptadores de red físicos en un único switch virtual y aislaremos las redes mediante el uso de redes de área local virtuales (VLAN). Utilizar VLAN [13] nos permitirá reducir los recursos físicos, pero compartiremos el caudal disponible sumando algo de gestión en la configuración de los switches físicos. Con esta configuración en cada host dispondremos de un único vSwitch estándar en el cual integramos todas las tarjetas de red activas y grupos de

puertos, permitiéndonos incrementar el ancho de banda y obteniendo alta disponibilidad. Debemos tratar de tener el menor número de vSwitches estándar que nos sea posible porque, de este modo, tendremos un mayor número de interfaces de red físicas para aplicar redundancia e incrementar el ancho de banda.

Una VLAN es un dominio de difusión configurado por software que permite crear redes agrupadas lógicamente, mejorando el rendimiento (al confinar el tráfico de difusión a un subconjunto de los puertos del switch) y ahorrando costes al particionar la red sin la sobrecarga que generarían nuevos routers. La VLAN ofrece la posibilidad de realizar una segregación del tráfico de red de forma lógica. Permite asignar un VLAN ID a los grupos de puertos del vSwitch estándar, permitiendo comunicaciones como si todas las máquinas virtuales o puertos de una VLAN estuviesen en el mismo segmento de LAN física. Por consiguiente, es posible tener en un mismo vSwitch infinidades de diferentes VLAN ID lo que hace tremendamente flexible un entorno de virtualización con VMware vSphere.

Los ESXi proporcionan soporte VLAN dando a un grupo de puertos un ID VLAN, a través del vSwitch estándar, y es el VMkernel el que se encarga de la asignación y desasignación de etiquetas a medida que los paquetes pasan a través del switch virtual.

Con todo lo analizado anteriormente y para cumplir con los aspectos importantes de diseño a nivel VMware, se va a disponer de dos tarjetas de red físicas activas por host, se va a crear un switch virtual estándar en cada uno de los 6 hosts físicos que componen la arquitectura virtual y se utilizan VLAN para realizar la segmentación de los distintos entornos funcionales. Contaremos con las siguientes VLAN en la red de la infraestructura virtual:

VM Port Group	VLAN ID
Red de gestión	10
Desarrollo	30
Webs	40
Preproducción	50
Producción	60
Servicios test	104
Administracion test	105
Base de datos test	106
Servicios producción	107
Administracion producción	108
Base de datos producción	109

Tabla 3: VLAN disponibles

La implementación de las VLAN se ha realizado teniendo en cuenta la creación de entornos de trabajo separados por las características de las aplicaciones, disponer de entornos para el acceso de proveedores, entornos para realizar pruebas, etc.

Para la configuración de la red Ethernet física vamos a utilizar dos switches de 48 interfaces en configuración de apilamiento para conseguir alta disponibilidad a nivel de red ethernet. Sobre estos switches se realizará la definición de las VLAN físicas definidas en la Tabla 3. Además, se definirá como puerto trunk* estático los puertos del switch físico donde irán conectados las interfaces de red físicas de los hosts ESXi. Para utilizar esta configuración, nuestros switch físico debe soportar el protocolo 802.1Q.

Los switches adquiridos para la configuración de la red ethernet física son dos switches de 48 puertos administrables, enracables y apilable modelo Allied Telesis STACK SW-AT8000gs/48. Sus principales características [14] son:

- 48 puertos 10/100/100.
- 4 puertos SFP 1000Base-X para conexiones utilizando fibra óptica.
- Administración sencilla a través de interfaz web segura y ssh.
- Configuración apilable en anillo con hasta 6 switches.
- Ofrecen soporte para la creación de VLAN hasta un máximo de 4096.
- Soporta EEE 802.1Q etiquetado VLAN

Para el control sobre el tráfico entre las distintas subredes con separación a través de VLAN y para el control de servicios hacia/desde Internet utilizaremos dos firewall en configuración de Alta disponibilidad. Además, los Firewall nos permiten proporcionar servicios al exterior y la comunicación con la plataforma virtual para su gestión, configuración, y administración de forma segura. Uno de los aspectos fundamentales de esta red es sin duda la seguridad. Los principales objetivos a conseguir son los siguientes:

- Seguridad y control en el acceso a internet. Control sobre todos los servicios publicados.
- Servicios de Antispam, Antivirus e IDS para la plataforma.
- Disponer de entornos funcionales de trabajo independientes.
- Disponer de acceso securizado para la gestión y administración de la plataforma. Servicios VPN y MPLS.
- Disponer de caminos seguros y con alta velocidad para la realización de backups remotos.

* Un puerto trunk es un puerto de un switch Ethernet físico que está configurado para enviar y recibir paquetes etiquetados con un identificador VLAN

La arquitectura de red virtual quedaría como se muestra en la siguiente figura:

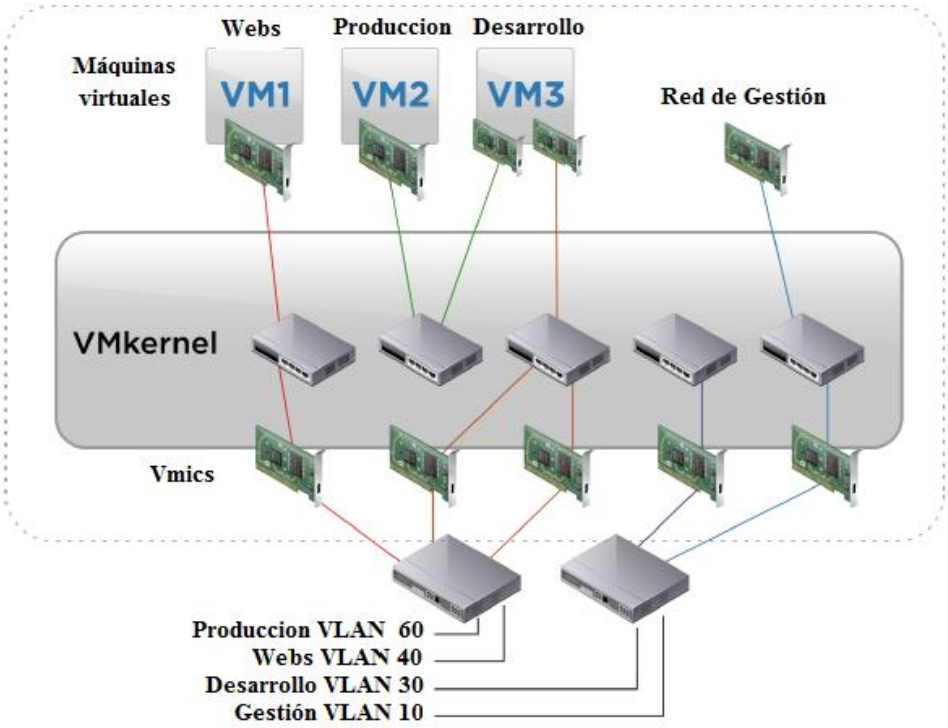


Figura 6: Arquitectura de red Ethernet virtual de la infraestructura

La arquitectura de red física diseñada quedaría como se muestra en la siguiente figura:

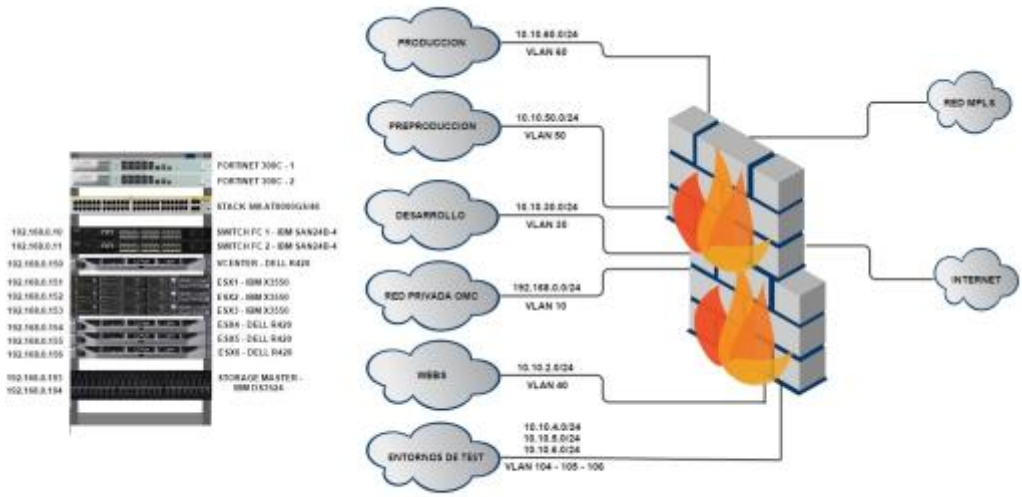


Figura 7: Arquitectura de red Ethernet física de la infraestructura virtual

3.5. Diseño de la red de Almacenamiento VMware vSphere

Una de las decisiones más importantes y críticas a la hora de diseñar una infraestructura de virtualización es la tecnología de almacenamiento a utilizar. Hay que destacar que, hoy en día, el principal activo de una empresa son sus datos. El diseño de almacenamiento va a determinar en gran medida el rendimiento de la infraestructura virtual. Para cualquier proceso de diseño de almacenamiento se consideran los siguientes requisitos:

Disponibilidad – Recuperación - Rendimiento – Administración - Seguridad

Debemos asegurar la alta disponibilidad en el almacenamiento para asegurar la continuidad de negocio en el centro de datos. Esto incluirá evitar cualquier punto único de fallo, así como también sistemas de recuperación con backups y réplica de datos. El rendimiento de nuestro sistema de almacenamiento será producto del conjunto de múltiples factores que serán de vital importancia de cara a un entorno ágil. Por otro lado, debemos conseguir un sistema de almacenamiento que sea controlable y administrable, y que esté aislado y securizado pues contendrá el activo más importante de la organización que son sus datos.

El principal factor limitante de todas las decisiones del proceso de análisis es, sin duda, el precio. La clave es encontrar el punto de equilibrio entre disponibilidad, rendimiento, escalabilidad y precio. A la vez que hacemos el análisis de lo que necesitamos debemos considerar el tiempo en que estimamos amortizar nuestra inversión. Entre 4 y 5 años suele ser un tiempo adecuado y prudencial. Una amortización menor a 4 años no será rentable y un tiempo superior a 5 años es muy posible que supere el tiempo máximo de soporte, recambios y actualizaciones del fabricante a la vez que la tecnología de almacenamiento se quedaría obsoleta.

3.5.1. Tecnología de almacenamiento

La primera decisión importante dentro del diseño del almacenamiento será seleccionar la tecnología de almacenamiento a utilizar. Para ello, realizamos un recorrido por las distintas tecnologías de almacenamiento disponibles [15], analizando en profundidad para ver cual se adapta mejor al uso en la plataforma virtual y a nuestro caso concreto. Además, como puede visualizarse en

la siguiente tabla, se analizaron las funcionalidades de la suite VMware vSphere que están disponibles con las diferentes tecnologías de almacenamiento:

Storage protocol	Supports boot from SAN	Supports VMware vSphere® vMotion®	Supports VMware vSphere® High Availability (vSphere HA)	Supports VMware vSphere® Distributed Resource Scheduler™ (DRS)	Supports raw device mapping (RDM)
Fibre Channel	•	•	•	•	•
FCoE	•	•	•	•	•
iSCSI	•	•	•	•	•
NFS		•	•	•	
DAS		•			•

Tabla 4: Funcionalidades vSphere con las tecnologías de almacenamiento (tomada de [1])

Como puede verse en la tabla anterior, VMware vSphere ofrece toda su funcionalidad disponible con la tecnología de almacenamiento SAN (*Storage Area Network*) en sus tres posibilidades de protocolo de transporte a utilizar: Fiber Channel, Fiber Channel sobre Ethernet(FCoE) y iSCSI.

Analizadas las diferentes tecnologías de almacenamiento y teniendo en cuenta que queríamos disponer de una arquitectura virtual que nos permitiera conseguir gran **rendimiento**, ya que teníamos aplicaciones con bases de datos de millones de registros; **escalabilidad**, que nos permitiera asumir el crecimiento de las aplicaciones y la introducción de otras nuevas; y las **máximas prestaciones** que nos pudiera ofrecer la virtualización con VMware vSphere, decidimos utilizar una red de almacenamiento dedicada SAN. La SAN es una tecnología de almacenamiento con una red dedicada que proporciona acceso al almacenamiento a nivel de bloque consolidado, y permite poner a disposición de los servidores, dispositivos de almacenamiento como matrices de discos, para que los dispositivos aparezcan como vinculados localmente al sistema operativo. La SAN dispone de una arquitectura completa que agrupa los siguientes elementos:

- Una red de alta velocidad que utiliza como protocolo de transporte Fiber Channel (FC), Fiber channel sobre Ethernet (FCoE), o iSCSI.
- Un equipo de interconexión dedicado (switches u otros dispositivos).
- Elementos de almacenamiento de red (discos duros).

Las redes SAN pueden ampliar fácilmente su capacidad casi de forma ilimitada pudiendo alcanzar miles de Terabytes. Además, pueden albergar diferentes tipos de disco, dependiendo de las necesidades que tengamos (rendimiento, capacidad, etc.), pudiendo convivir en un mismo sistema tanto discos SAS, como SSD, Flash (FMD) o NL-SAS. Al no utilizar la LAN corporativa, elimina la competencia por los recursos de red, lo que contribuye a reducir la posibilidad de tiempos de

respuesta largos e impredecibles. Además, permite realizar backups de servidores con poco impacto en los servidores de aplicaciones, aumentar la frecuencia de estas operaciones, y efectuar restauraciones actualizadas en menos tiempo. La principal desventaja de la SAN es sin duda que el coste económico de implantación y el mantenimiento es más elevado. Además, introduce una mayor complejidad en la arquitectura y la administración del almacenamiento a desplegar, al incluir más elementos adicionales necesarios.

Como protocolo de transporte de la red SAN se descartó desde el primer momento FCoE por el precio desorbitado en la implantación y la complejidad en la gestión. Entre las tecnologías restantes se decidió utilizar Fiber Channel por las razones expuestas a continuación [16][17]:

1) Experiencia ya adquirida en redes SAN con Fiber Channel, tecnología que ya habíamos utilizado en el almacenamiento de la arquitectura formada por servidores del fabricante Apple, que ya estaba disponible en mi empresa.
2) Fiber Channel ofrece un grado alto de rendimiento y fiabilidad. En redes SAN que utilizan tecnología Fiber Channel se consiguen altos anchos de banda y gran estabilidad.
3) La red SAN con Fiber Channel ofrece una red de almacenamiento exclusiva totalmente aislada e independiente de la red de tráfico TCP/IP de gestión y prestación de servicios. En Fiber Channel e iSCSI se consiguen velocidades máximas de transmisión similares. Sin embargo, en una red SAN Fiber Channel no afecta el trabajo de los usuarios al no compartir la red Ethernet y además consigue ínfimo número de paquetes perdidos en la transmisión aumentando el ancho de banda.
4) Otro aspecto importante a tener en cuenta es la seguridad. Al tener la red de almacenamiento separada de la red Ethernet, una tormenta de *broadcast* o cualquier problema de seguridad en la red no afecta al acceso de almacenamiento, lo que provoca que no haya pérdida de servicio para procesos internos y no se produzcan corrupciones en el almacenamiento de los datos.
5) Si la carga transaccional de las bases de datos es muy elevada (muchas peticiones pequeñas simultáneas), el rendimiento que consigue iSCSI es peor que al utilizar tecnología Fiber Channel. iSCSI tiene mayores problemas con aplicaciones que tengan demanda alta de accesos entrada/salida, no grandes bloques de datos, sino en peticiones de datos pequeños de forma continua que requieren operaciones de bases de datos como *commit* o *rollback* (OLTP). En este escenario, iSCSI genera mayor carga de procesamiento que tener tarjetas HBA* dedicadas con una red SAN basada en Fiber Channel.

* HBA(*Host Bus Adapter*): tarjeta que permite conectar un equipo con un sistema de almacenamiento a través de fiber channel

El principal inconveniente de utilizar la tecnología Fiber Channel con respecto a la tecnología iSCSI es el de mayor coste económico que exige, derivado de la necesidad de adquirir elementos exclusivos para la red SAN Fiber Channel como son los switches Fiber Channel o las tarjetas HBA (*Host Bus Adapter*). Sin embargo, en mi empresa los switches Ethernet disponibles en ese momento trabajaban a velocidad máxima de 1Gb por lo que en el caso de elegir la tecnología iSCSI deberíamos adquirir nuevos switches Ethernet de mayores prestaciones para poder conseguir velocidades de trabajo superiores y, de este modo, el desembolso en la compra de switches también debería ser realizado.

Otro inconveniente conocido es la mayor complejidad en la gestión de la SAN Fiber Channel, pero en nuestro caso esto no sería un inconveniente porque ya teníamos experiencia adquirida en la gestión de redes SAN con Fiber Channel como protocolo de transporte.

Por los motivos expuestos anteriormente y dado que nuestras aplicaciones requieren una demanda alta de accesos entrada/salida, como por ejemplo consulta masiva de recetas o certificados electrónico, fueron razones que llevaron a decantarse por utilizar Fiber Channel como protocolo de transporte de nuestra red SAN.

En la figura 8 pueden verse los componentes típicos de una SAN que utiliza Fiber Channel:

Figura 8: Componentes típicos de una SAN FC (tomada de [1])

Los componentes típicos de una red SAN Fiber Channel son:

- Sistema de almacenamiento: consiste en un conjunto de discos duros físicos y uno o varios controladores inteligentes. El sistema de almacenamiento admite la creación de LUN (*Logic Unit Number*), que es básicamente un disco virtual. Un LUN es un espacio de disco en bruto (sin formato) que presenta un sistema de almacenamiento (SAN) a uno o varios Hosts. El uso

de LUN simplifica la administración de los recursos de almacenamiento de la red SAN porque sirven como identificadores lógicos que permiten asignar privilegios de acceso y control. Los procesadores de almacenamiento de las matrices de discos concentran discos físicos en LUN, cada uno de ellos con su identificador de LUN.

- HBA: adaptador de bus de host. Conecta el host ESXi a la red de Fiber Channel. El HBA es necesario y debe estar conectado mediante cables de Fibra a los puertos de switch de Fiber Channel. Para las configuraciones con tolerancia a fallos se utilizan dos adaptadores HBA como mínimo.
- Switch Fiber Channel: se encargan de la interconexión de varios nodos y la estructura SAN. Suele usarse varios para permitir redundancia y alta disponibilidad en el acceso a los datos. Añaden direcciones de origen y destino a cada paquete.

3.5.2. Red SAN de la infraestructura virtual

Con todas las consideraciones anteriores diseñamos la arquitectura de nuestro almacenamiento como se muestra en la siguiente figura:

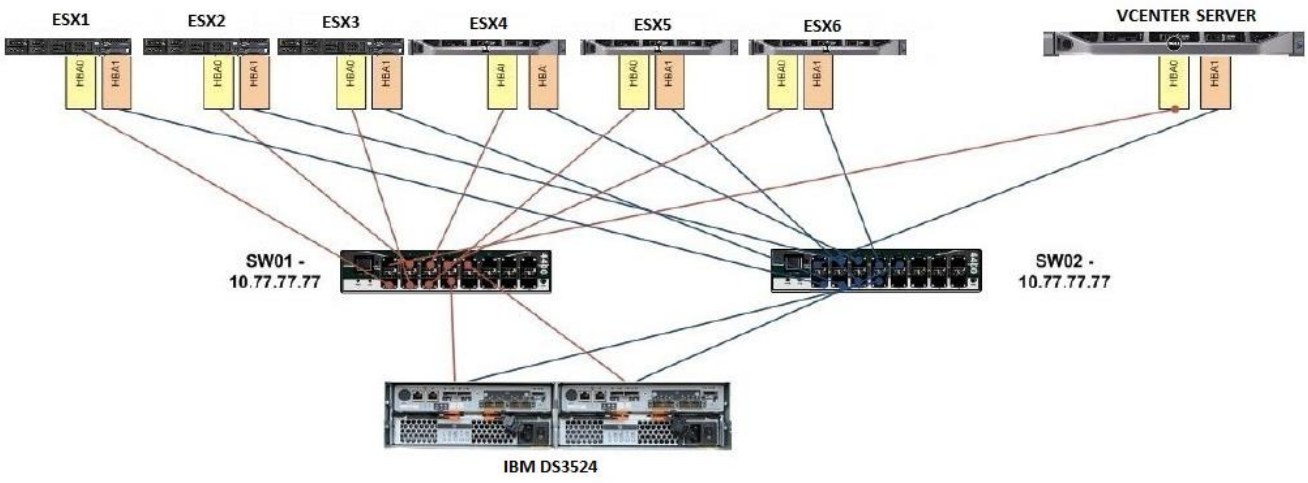


Figura 9: Arquitectura de la red SAN

En la imagen anterior puede verse la red de almacenamiento dedicada de la arquitectura virtual de mi empresa. Los elementos que componen la SAN diseñada son descritos a continuación:

Sistema de Almacenamiento:

Cabina IBM System Storage DS3524 *Express Dual Controller* modelo C4A [18][19]. Las características más importantes son:

La cabina IBM DS3524 dispone de conectividad (SAS) a nivel de disco y soporta los niveles de RAID 0, 1, 3, 5, 6 y 10. Soporta configuraciones de discos SAS de 6Gbps, SAS NL, discos de estado sólido (SSD), SAS 6Gbps *Full Disk Encryption* (FDE) o combinación de las posibilidades anteriores. Dispone de una capacidad máxima de 24 TB que utilizaremos al completo mediante la colocación de de 24 discos de 1 TB 2.5in 7.2K 6Gb NL SAS.

La cabina IBM DS3524 es un sistema de almacenamiento enracable de 2U que dispone de dos controladoras de almacenamiento RAID redundantes activas simultáneamente. La **redundancia en controladora** es realmente importante no solo por incrementar la disponibilidad, sino que también ayuda a distribuir la carga. Las dos controladoras funcionan en activo-activo de forma que vamos a disponer de servicio de forma simultánea lo que nos aportará una mayor versatilidad a la hora de distribuir la carga. Cada controladora dispone de dos puertos de interfaz host SAS a 6Gbps y dispone de una tarjeta para añadir nuevos puertos de interfaz host (que deben ser del mismo tipo en ambas controladoras). Cada controladora dispone además de 1 puerto ethernet y de 1GB de memoria caché que puede ser ampliada a 2 GB. La caché de la cabina puede mejorar notablemente el rendimiento moviendo a la caché los bloques de memoria más consultados.

Dentro de la cabina DS3524 existen funciones de gestión de almacenamiento avanzada, copias de configuración y funciones avanzadas de recuperación de desastres como son *FlashCopy*, *VolumeCopy* y *Enhanced Remote Mirroring*:

- *FlashCopy® and Volume Copy* se utilizan para crear copias de datos física o lógicas.
- *Remote Mirroring* se utiliza para replicación de datos hacia otra cabina de la serie DS3500 a través de comunicaciones basadas en enlaces Fiber Channel usando transferencias de datos síncronas o asíncronas. Esta característica la utilizaremos en nuestra arquitectura para la replicación de los datos de la cabina principal dentro de nuestra política de recuperación de desastres y continuidad de negocio. El diseño e implementación de esta solución de almacenamiento redundante será abordada en detalle en el capítulo 6.

Switches Fiber Channel:

Express IBM System Storage SAN24B-4 [20]:

Disponemos de dos switches FC modelo Express IBM System Storage SAN24B-4. Está diseñado especialmente para atender las necesidades de los entornos de red de área de almacenamiento (SAN)

de tamaño pequeño a medio. La configuración estándar incluye la activación de 8 puertos y la capacidad de conectarse a sistemas hosts y a dispositivos de almacenamiento. Dispone de la denominada función de puertos *on demand* que ofrece una escalabilidad que permite ampliar un switch base a 16 y 24 puertos con el fin de admitir más servidores y más dispositivos de almacenamiento sin tener que desconectar el switch. Este switch permite crear una solución de alta disponibilidad mediante switches redundantes, función ideal para nuestro entorno y que nos permitiría admitir de 6 a 22 servidores, cada uno con adaptadores fiber channel duales, HBAs, conectados de forma cruzada a switches SAN24B-4, conectados a su vez de forma cruzada a un sistema de almacenamiento con controladora dual. Las principales características del switch son expuestas a continuación:

- Diseño de 1U para montaje en bastidor.
- Proporciona capacidad de auto detección de velocidad y trabaja a una velocidad máxima de 8 Gbps (requiere hardware de almacenamiento que trabaje a esa velocidad). Permite también velocidades de 4,2 y 1 Gbps.
- Compatibilidad con transceptores ópticos de onda corta y larga y su sustitución de forma sencilla en caliente.
- No se necesita experiencia previa en SAN para usar el asistente de instalación y gestión *EZSwitchSetup*.
- La herramienta Advanced Web Tools permite una gestión de switch gráfica e intuitiva a través de cualquier navegador.
- La función estándar *Advanced Zoning* proporciona *zoning*[*] mediante hardware como protección ante accesos a la red de almacenamiento no autorizados o no autenticados
- Tiene a su disposición acceso y gestión remota a través de telnet.

En cada switch Fiber Channel IBM System Storage SAN24N-4 adquirido vienen activados de fábrica 8 puertos y se ha necesitado activar otros 8 puertos adicionales, para disponer de 16 en total en cada switch, para poder dar servicio a las tarjetas duales HBA de cada uno de los 7 servidores físicos más las conexiones de cada una de las controladoras de la cabina de almacenamiento, necesitando nueve SFP 8 Gbps SW para cada uno de los switches. El hecho de adquirir la activación de 8 puertos adicionales a pesar de necesitar solo uno es debido a que la activación de puertos adicionales se licencia en paquetes de ocho puertos. Los puertos restantes adquiridos podremos utilizarlos si damos

[*] El *zoning* es un concepto exclusivo de las redes SAN Fiber Channel y lo analizaremos en profundidad en la sección 4.4, donde se explicará la configuración de los switches Fiber Channel de la infraestructura virtual.

escalabilidad a la solución o conectamos elementos de almacenamiento adicionales. Además, para cada switch se ha adquirido la licencia para el funcionamiento en *Full Fabric*, que es la licencia recomendada por el fabricante para la arquitectura de la red SAN mostrada en la figura 9. Esta licencia permite conectar un switch FC a otros múltiples switches FC mediante los llamados puertos de expansión formando conexiones denominadas *interswitch* o ISL, y permitiendo arquitecturas SAN con múltiples switches FC funcionando ordenadamente. La interconexión de uno o más switches dentro de una topología de red SAN se conoce como *Fabric*.

Tarjetas para las comunicaciones Fiber Channel [21]:
Dispondremos de siete tarjetas QLogic 8Gb FC Dual-port HBA for IBM System X para los hosts y el Vcenter Server y dos tarjetas 8Gb FC 4 Port para la cabina de almacenamiento IBM DS3524. En este punto tuvimos que consultar al fabricante IBM la compatibilidad de sus tarjetas con los servidores DELL y la respuesta fue afirmativa.

Cableado de comunicaciones Fiber Channel:
El cableado de conexión Fiber Channel que puede utilizarse con la cabina puede ser de 1, 5 y 25 metros [18]. Para nuestra red SAN utilizamos cableado FC de 5m de elevadas prestaciones.

El acceso a la SAN se proporcionará a nivel de LUN. Según esto, en la cabina de almacenamiento se crearán las unidades de almacenamiento, LUN, para presentarla a los servidores ESXi con el propósito de albergar los discos de las máquinas virtuales, los ficheros de configuración, imágenes del estado de las máquinas virtuales y los ficheros de Log. Toda esa información es respaldada por el kernel de ESXi, utilizando un sistema de ficheros llamado VMFS, que es el sistema de fichero de VMware. Las LUN se presentarán en modo lectura/escritura a todos los ESX, para que puedan acceder concurrentemente a ellas.

VMware tiene dos métodos bien diferenciados a la hora de configurar el tamaño correcto para las LUN de almacenamiento: el método predictivo y el método adaptativo. El método adaptativo utiliza menos LUN, pero más grandes mientras que el método predictivo utiliza varias LUN con diferentes tipos de RAID para ajustarse mejor a las características de E/S de las diferentes aplicaciones. Las mejores prácticas de VMware [9] en cuanto a la ubicación de la máquina virtual en las LUN indican que lo óptimo es crear LUN de 600 a 1000 Gb que alberguen de 10 a 12 máquinas virtuales. El tamaño máximo de LUN que permite VMware vSphere 5 es 2 TB. Sin embargo, luego en la práctica veremos que a la hora de albergar una nueva máquina virtual en una

LUN debemos monitorizar el retardo que va a provocar la entrada de la nueva máquina para evitar cuellos de botella. La apuesta de diseño suele ser crear más LUN de un tamaño medio para tratar de distribuir de forma adecuada las máquinas virtuales en ellas y evitar que la pérdida de una LUN afecte a muchas máquinas virtuales que estaban alojadas en ella.

3.5.3. Sistema de archivos de VMware

Finalmente, para cerrar este apartado abordaremos el sistema de archivos específico de VMware. VMware vSphere VMFS es el sistema de ficheros que utiliza VMware y está diseñado, creado y optimizado para el entorno virtualizado [1]. Los sistemas convencionales no permiten que varios servidores tengan acceso de lectura y escritura a un archivo determinado al mismo tiempo. Por este motivo se creó VMFS que permite a los mismos hosts ESXi acceder simultáneamente a los mismos recursos de almacenamiento compartido con permisos de lectura y escritura. Se trata de un sistema de ficheros en clúster de alto rendimiento diseñado para las máquinas virtuales que usa un registro distribuido para los cambios en los metadatos de su sistema de archivos, lo que permite una recuperación rápida y fiable en caso que falle el hardware. Las características que proporciona VMFS permiten la migración en caliente de máquinas virtuales y sus archivos, balanceo dinámico de cargas de trabajo, reinicio automático de máquinas virtuales y tolerancia a fallos. VMFS proporciona una interfaz para los recursos de almacenamiento, de forma que pueden usar diversos protocolos de almacenamiento de transporte en el almacenamiento: Fiber Channel, Fiber Channel sobre Ethernet, iSCSI y NAS). VMFS:

- Permite el acceso simultáneo a almacenamiento compartido.
- Puede ampliarse dinámicamente.
- Usa un tamaño de bloque de 1MB, adecuado para almacenar archivos grandes de discos virtuales.
- Ofrece bloqueo en disco a nivel de bloque, lo que permite hacer clones o snapshot de máquinas virtuales.

No hay ningún otro sistema de archivos en clúster que ofrezca la funcionalidad de VMFS. Sus métodos de bloqueo distribuido forman el enlace entre la máquina virtual y los recursos de almacenamiento subyacentes de forma tal que ningún otro sistema de archivos en clúster ha

conseguido igualarlo. La funcionalidad única de VMFS permite que las máquinas virtuales se unan a un clúster sin interrupciones y sin sobrecarga de gestión.

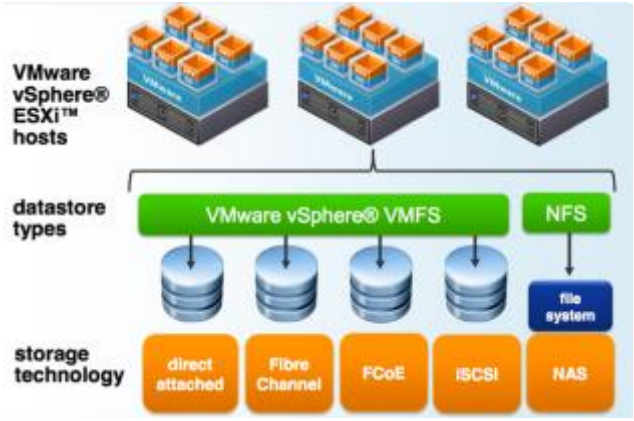


Figura 10: Sistema de fichero VMFS de VMware (tomada de [1])

VMFS almacena todos los archivos que componen la máquina virtual en un solo directorio. Cada *datastore* se monta en una carpeta y contiene varios subdirectorios con los archivos que describen a la máquina virtual. VMFS proporciona encapsulación de toda la máquina virtual, de modo que puede así utilizarse como parte de una solución de continuidad de negocio o de recuperación de desastres.

3.6. Resumen y conclusiones

En este capítulo se ha realizado el diseño de los aspectos más importantes de la arquitectura virtual:

- El objetivo es poder desplegar un mínimo de 40 máquinas virtuales que den servicio a los proyectos actuales de la empresa y los proyectos a implantar, dando cobertura a los diferentes entornos de producción, preproducción o pruebas.
- Para ello, se decide usar 6 servidores hosts ESXi que van a componer el clúster de servidores físicos de la infraestructura virtual. Se ha dimensionado de modo que el clúster permita la caída de un host físico y tengamos una capacidad de escalabilidad del 20%.
- Se usa un servidor dedicado que va a albergar el VMware Vcenter Server para la gestión y administración centralizada de la plataforma.
- Para dar cobertura de licencias al clúster, se han adquirido licencias VMware vSphere 5 versión Standard para licenciar 12 procesadores físicos y se ha adquirido una licencia de VMware Vcenter Server Standard.

- El pool de recursos de CPU y memoria RAM con los que se ha dimensionado el clúster de forma inicial son 12 procesadores físicos y 144 GB de RAM físicos. El recurso de la RAM es fácilmente escalable mediante la inclusión de módulos en los servidores físicos hasta un máximo de 384 GB, 64 GB por ESXi, límite que nos marca la licencia VMware vSphere Standard 5.
- El diseño de la red ethernet se ha realizado de modo que vamos a configurar un switch virtual estándar por cada host ESXi del clúster. Además, para garantizar la alta disponibilidad a nivel de red, dispondremos de 2 tarjetas de red físicas activas por cada host ESXi. Finalmente vamos a utilizar VLAN para definir diferentes entornos funcionales de trabajo para segurizar y optimizar el funcionamiento de los servicios.
- El almacenamiento en la infraestructura virtual se basa en una red SAN con tecnología Fiber Channel con redundancia en el acceso al almacenamiento, usando una cabina IBM con redundancia en controladora y 24 TB de capacidad bruta. Esta capacidad será organizada en LUN y contará con el sistema de archivos VMFS.

Capítulo 4:

4. Implantación de la arquitectura de virtualización

En este capítulo se va a describir detalladamente el proceso de implantación del diseño de la arquitectura virtual basada en VMware definida en el capítulo anterior.

4.1. Instalación y configuración de la red Ethernet

En este apartado vamos a describir el proceso para la configuración de la red ethernet física sobre la que se va a sustentar la red ethernet de la arquitectura virtual. La configuración de la red ethernet física se debe realizar para permitir el diseño de la red ethernet de la arquitectura virtual que se describió en el apartado 3.4.

La piedra angular de la configuración de la red ethernet serán los switches ethernet con configuración en apilamiento que permitirá disponer de la división funcional en VLAN de los diferentes entornos funcionales a crear, alta disponibilidad a nivel de máquina virtual que nos proporcionará la red de gestión VMware vSphere, 5 y la redundancia de servicios disponibles hacia internet. Para lograrlo conectaremos cada una de las 2 interfaces de red físicas, que tiene activas cada ESXi, a cada uno de los dos switches ethernet.

La primera tarea a realizar para la configuración de la red Ethernet es la instalación de los dos switches Allied Telesis 8000GT/48. Para ello seguimos la documentación del fabricante que se incluye en los puntos de bibliografía [22] [23].

El procedimiento a seguir sería el siguiente:

1) Instalación física de los switches: desempaquetamos y enracamos los dos switches en el bastidor de nuestro CPD.
2) Conectamos los switches a la red eléctrica y los arrancamos.
3) Realizamos la configuración inicial. Para ello:

En primer lugar, hay que tener en cuenta que, para obtener la alta disponibilidad a nivel de switch, se realizará una configuración de los mismos en apilamiento (stack). Para ello unimos ambos switches con una conexión de alta velocidad (interfaz HDMI) conectando los denominamos *stacking ports* de la parte trasera de ambos switches. Esto permite que ambos switches sean administrados a través de una única IP a través línea de comando (CLI), interfaz web o gestión SNMP. La siguiente imagen muestra la configuración en *stack* que se ha realizado con los dos switches disponibles:

```
console# show stack
Unit  MAC Address        Software    Master    Uplink     Downlink   Status
----  -----------------  ----------  --------  ---------  ---------  -------
1     ec:cd:6d:b4:a7:bd  2.0.0.27    Enabled   2          2          master
2     ec:cd:6d:b4:99:00  2.0.0.27    Enabled   1          1          backup
Topology is Ring

Unit Unit Id After Reset
---- -------------------
 1            1
 2            2
```

Figura 11: Configuración stack de los switches Ethernet AT8000GT/48

Siguiendo la documentación del fabricante, creamos el grupo para el apilado de los switches y unimos a ambos al *stack*. La configuración en apilado se realiza interrumpiendo el arranque de los switches y añadiendo estos al stack mediante un menú destinado a ello. Cuando finaliza la configuración, al arrancar los switches estos serán configurados dentro del apilado creado como un único punto de administración y configuración.

Una vez que ambos dispositivos se han definido dentro del *stack*, comenzaremos la configuración inicial del switch máster y, desde aquí, se replicará automáticamente al otro switch. Para ello nos conectamos al switch máster a través de un terminal utilizando un puerto de consola situado en la parte posterior de dicho switch. La conexión de la consola permite disponer de una conexión a un terminal de escritorio donde se ejecuta un software de emulación de terminal para la monitorización y la configuración del dispositivo.

Figura 12: Conexiones parte trasera del switch AT8000GT/48

El puerto de consola situado en el panel posterior es un puerto con conexión RJ45 que soporta la especificación eléctrica RS-232. Para conectar un terminal al puerto de dispositivo de consola realizamos el siguiente procedimiento:

a) Conectar el cable al puerto de consola. Para conectarnos utilizamos un cable RJ45 que soporte las especificaciones eléctricas RS-232.

b) Conectar el otro extremo del cable al PC donde se está ejecutando el software de emulación de terminal VT100.

c) Configuramos el hyperterminal con los siguientes parámetros:

- Ajustar la velocidad de datos de 115.200 baudios.
- Ajustar el formato de datos a 8 bits de datos, 1 bit de parada y sin paridad.
- Establecer el control de flujo en ninguno.
- En Propiedades, seleccione modo de emulación VT100.
- Seleccionar teclas del terminal para Función, Flecha y teclas Ctrl. Asegurarse de que el ajuste es para teclas de terminal (no las teclas de Windows).

d) Presionamos enter y colocamos las credenciales de acceso por defecto que nos proporciona el fabricante (manager/friend).

e) De este modo ya disponemos de acceso local al switch.

Tras esto, comenzamos la configuración inicial del switch. Tras realizar cualquier modificación en la configuración del dispositivo, la nueva configuración debe ser guardada antes de reiniciar el mismo. Para guardar la configuración, se utiliza el siguiente comando CLI:

Console# copy running-config startup-config

La configuración inicial, que comienza después de que el dispositivo ha arrancado con éxito, incluye la dirección IP estática, la configuración de la máscara de subred y el establecimiento de nombre de usuario y nivel de privilegio para permitir la gestión remota. Por ello, lo primero que haremos es fijar al switch una IP fija y una máscara de subred utilizando los comandos CLI destinados para ello. Tras ello, la configuración queda como se muestra en la siguiente figura:

```
console# show ip interface

  Gateway IP Address        Activity status       Type
---------------------- ---------------------- --------
172.31.250.1           Active                  static

     IP Address                I/F            Type
---------------------- -------------------- ---------
172.31.250.4/24         vlan 1               Static
```

Figura 13: Configuración inicial del switch AT8000GT/48

Para la gestión remota del switch, a través de SSH, Telnet o interfaz web, definiremos unas credenciales de acceso seguras. Por ello, fijamos una contraseña segura para el usuario de administración del dispositivo que en este caso es el usuario **manager**. Para ello utilizamos los comandos CLI que nos indica el fabricante (*Console# username manger password lee privilege 15)*

Tras arrancar el switch con la configuración inicial ya dispone de una IP fija a través de la cual podemos administrar y configurar dicho dispositivo mediante SSH, Telnet o interfaz web.

4) Actualización del firmware de los switches FC a la última versión publicada por el fabricante. Las mejores prácticas recomiendan que ambos switches dispongan de la misma versión de firmware.
5) Realización la configuración completa de los switches Ethernet.

   Para la realización de la configuración avanzada de los switches, así como la definición de las diferentes VLAN y direccionamiento de las mismas, utilizamos tanto la interfaz de comandos CLI, a través de conexión telnet a los switches, como la configuración a través de la interfaz web a través de navegador. A través de ambos métodos de conexión y, utilizando las credenciales de acceso segura, definimos la configuración de los switches. Cabe resaltar que los comandos utilizados son muy similares a los utilizados para la configuración de dispositivos CISCO.

   En primer vamos a determinar los dos tipos de puertos, o modos de acceso a los mismos, que vamos a configurar en los switches dependiendo del uso que se le vaya a dar a la VLAN a la que pertenece dicho puerto:

	#	Interface	Interface VLAN Mode	PVID	Frame Type	Ingress Filtering	Reserved VLAN
○	1	1/g1	Access	501	Admit All	Enable	
○	2	1/g2	Access	501	Admit All	Enable	
○	3	1/g3	Access	502	Admit All	Enable	
○	4	1/g4	Access	502	Admit All	Enable	
○	5	1/g5	Access	1	Admit All	Enable	
○	6	1/g6	Access	1	Admit All	Enable	
○	7	1/g7	Access	10	Admit All	Enable	
○	8	1/g8	Access	40	Admit All	Enable	
○	9	1/g9	Trunk	20	Admit All	Enable	
○	10	1/g10	Access	50	Admit All	Enable	
○	11	1/g11	Access	30	Admit All	Enable	
○	12	1/g12	Access	60	Admit All	Enable	
○	13	1/g13	Trunk	1	Admit All	Enable	
○	14	1/g14	Trunk	1	Admit All	Enable	
○	15	1/g15	Access	10	Admit All	Enable	
○	16	1/g16	Access	10	Admit All	Enable	
○	17	1/g17	Access	10	Admit All	Enable	
○	18	1/g18	Access	10	Admit All	Enable	
○	19	1/g19	Access	10	Admit All	Enable	
○	20	1/g20	Access	10	Admit All	Enable	
○	21	1/g21	Trunk	1	Admit All	Enable	
○	22	1/g22	Trunk	1	Admit All	Enable	
○	23	1/g23	Trunk	1	Admit All	Enable	
○	24	1/g24	Trunk	1	Admit All	Enable	

○	25	1/g25	Trunk	1	Admit All	Enable	
○	26	1/g26	Trunk	1	Admit All	Enable	
○	27	1/g27	Access	10	Admit All	Enable	
○	28	1/g28	Access	10	Admit All	Enable	
○	29	1/g29	Access	10	Admit All	Enable	
○	30	1/g30	Access	10	Admit All	Enable	
○	31	1/g31	Access	10	Admit All	Enable	
○	32	1/g32	Access	10	Admit All	Enable	
○	33	1/g33	Access	10	Admit All	Enable	
○	34	1/g34	Access	10	Admit All	Enable	
○	35	1/g35	Access	10	Admit All	Enable	
○	36	1/g36	Access	10	Admit All	Enable	
○	37	1/g37	Access	10	Admit All	Enable	
○	38	1/g38	Access	10	Admit All	Enable	
○	39	1/g39	Access	10	Admit All	Enable	
○	40	1/g40	Access	10	Admit All	Enable	
○	41	1/g41	Access	20	Admit All	Enable	
○	42	1/g42	Access	20	Admit All	Enable	
○	43	1/g43	Access	40	Admit All	Enable	
○	44	1/g44	Access	40	Admit All	Enable	
○	45	1/g45	Access	40	Admit All	Enable	
○	46	1/g46	Access	40	Admit All	Enable	
○	47	1/g47	Access	1	Admit All	Enable	
◉	48	1/g48	Access	1	Admit All	Enable	

Figura 14: Configuración puertos trunks switches AT8000GS/48

En la figura anterior pueden verse la configuración de los puertos realizada en los switches a través del acceso web. Puede visualizarse los dos modos de interfaz VLAN que pueden configurarse: acceso (Access) y troncales (*Trunk):*

- Modo *acceso*: Permite una sola VLAN, los paquetes no van etiquetados y están destinados para conectar dispositivos finales. Permiten el acceso de los dispositivos finales a la red a través del switch. Se utilizará para gestionar el tráfico de las máquinas virtuales que pertencezca a esa VLAN.
- Modo *troncal*: Permite gestionar el tráfico de varias VLAN en un mismo puerto, por lo que los paquetes irán etiquetados, siguiendo el estándar IEEE 802.1Q (dot1q), para determinar la VLAN destino. Se utiliza para interconectar distintos switches y, en nuestro caso, se utilizará para conectar los switches físicos a los switches virtuales para canalizar el tráfico de las distintas VLAN pertenecientes a los distintos entornos funcionales diseñados.

El valor por defecto de los puertos es *General*, que indica que el puerto soporta VLAN con encapsulamiento 802-1q. Para configurar el modo de interfaz VLAN en estos puertos se puede utilizar la interfaz de configuración web o siguiendo los comandos recomendados por VMware para los switches de tipología CISCO utilizando la interfaz de comandos CLI. Otro dato a destacar en la figura anterior es el VLAN ID (PVID) que determina la VLAN a la que pertenece cada puerto. La VLAN cuyo VLAN ID es 1 es la VLAN nativa del switch AT8000GS/48. La configuración de las VLAN es mostrada en la siguiente tabla:

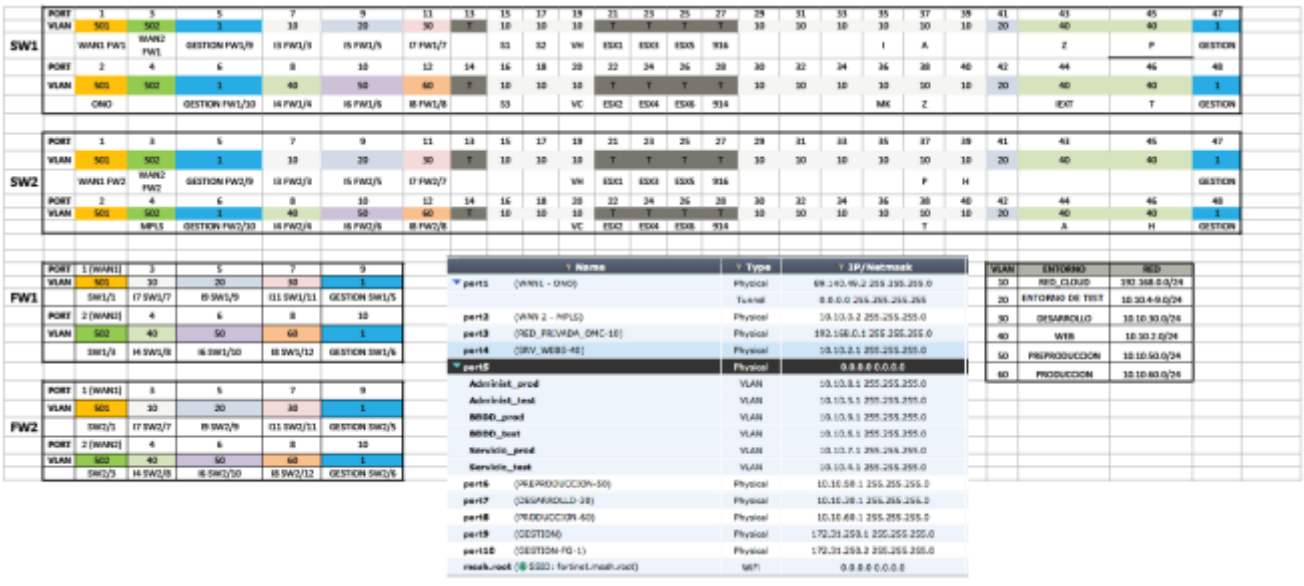


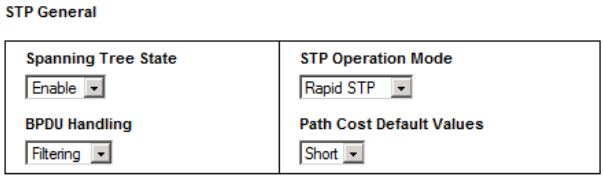
Figura 15: Configuración avanzada de los switches AT8000GS/48

Se ha optado por resumir las configuraciones realizadas en los switches en la tabla Excel anterior en lugar de mostrar capturas de pantalla de las configuraciones que ofrecen tanto la interfaz web como la interfaz de comandos de los switches con el fin de comprimir la presentación de la información en una sola imagen, ya que de lo contrario exigiría la emisión de múltiples capturas de pantalla para mostrar toda la información recogida anteriormente, y dicha información no se presentaría de forma tan clara y concisa. Para elaborar la tabla anterior se ha utilizado precisamente la información que se desprende de consulta por línea de comando o interfaz web a los switches tras su configuración.

En la figura anterior se muestra la configuración realizada en cada uno de los puertos de cada switch Ethernet. Pueden verse las distintas VLAN creadas, la conectividad en los puertos troncales (trunks), la conectividad con los dispositivos Firewall, y la conectividad con algunos servidores físicos que están fuera de la arquitectura virtual. A continuación se explica con detalle la figura anterior:

- Los puertos de los switches etiquetados en la gráfica con "T" (13,14,21-28) son los puertos configurados como troncales y es donde se conectarán los hosts ESXi. Los puertos utilizados para conectar los ESXi han de permitir, únicamente, el paso de las VLAN que se han configurado en la infraestructura virtual. La razón de utilizar este tipo de puertos es para interconectar el switch físico con los switches virtuales que se creen en los ESXi en la arquitectura virtual y, de este modo, comunicar las máquinas virtuales con los switches físicos y con el exterior. Para la configuración completa para el etiquetado VLAN necesario dentro de los puertos troncales que utilizarán los host ESXi se debe seguir el siguiente procedimiento [24]:

  - Configurar el puerto físico al modo troncal.
  - Habilitar la encapsulación dot1q. Esta se habilita automáticamente al configurar un puerto como troncal.
  - Configurar el Rapid Spanning Tree Protocol (RSTP).



  - Definir la interfaz de VLAN. Tendrá el VLAN ID 1, que es la VLAN nativa del switch.

- Asignar el rango de IP a la interfaz de VLAN. El direccionamiento utilizado la VLAN 1 es 172.31.250.0/24.
- Enrutamiento y aislamiento de VLAN. Definimos el gateway y la máscara de subred.

En switches Allied Tellesis, la VLAN nativa es la VLAN por la que circula el tráfico de protocolos de nivel 2, y la que no tiene un etiquetado de VLAN. En la configuración de etiquetado de VLAN, el ESXi no admite el ID nativo de VLAN. Por este motivo, todos los grupos de puertos han de tener un VLAN ID y este debe ser distinto a la VLAN nativa, para prevenir que algún tráfico se cuele en la VLAN nativa en vez de circular por la VLAN que le toca. Todos los puertos que no son troncales, tienen configurado el modo acceso y pertenecerán a una determina VLAN identificada con un VLAN ID.

- Los puertos que aparecen en la figura 15 etiquetados con VLAND ID 501 y 502 son utilizadas para conexiones WAN.
- Los puertos de cada switch número 5, 6, 47 y 48 se utilizan para la administración externa remota de la arquitectura de comunicaciones a través de un clúster de dispositivos Firewall en alta disponibilidad. Estos puertos están dentro de la VLAN nativa del switch con VLAN ID 1.
- El resto de puertos están etiquetados con el identificador de la VLAN a la que pertenecen, que ya se había definido en el diseño y que se resumen en la siguiente tabla:

VLAN ID	ENTORNO	RED
10	Red de gestión VMware	192.168.0.0/24
20	Entornos de tests	10.10.4-9.0/24
30	Desarrollo	10.10.30.0/24
40	Webs	10.10.2.0/24
50	Preproducción	10.10.50.0/24
60	Producción	10.10.60.0/24

Tabla 5: Descripción VLAN

- Los puertos comprendidos entre el 35 y el 46 de cada switch son utilizados para conectar servidores físicos que ofrecen servicios que serán migrados a la infraestructura virtual tras finalizar la implantación de esta.

Cabe resaltar que los puertos 7, 8, 9, 10, 11 y 12 de cada switch van conectados a las interfaces de un Firewall, con configuración en clúster en alta disponibilidad. Este firewall, a través de estos puertos, está conectado a todas las subredes y actúa de gateway en todas y cada una de ellas. De este modo, permite definir las políticas de tráfico entre los distintos entornos funcionales definidos por las

VLAN, y el tráfico entre estos entornos y las redes WAN(*Wide Area Network*), a través de la VLAN 501 y 502 . Nos permite de este modo proporcionar seguridad a la plataforma.

6) Conexión del cableado Ethernet físico entre los switches y las tarjetas de red de los distintos dispositivos a conectar. Todas las conexiones de cableado ethernet se han realizado con cables Ethernet RJ45 de 1,5 metros de longitud de categoría 7.
7) Verificación de la configuración.
   Para finalizar la configuración verificamos que la configuración del switch es la deseada. Para ello verificamos el correcto funcionamiento de los siguientes parámetros:

- La velocidad de los puertos.
- Verificamos la configuración general de los switches.
- Verificamos la conectividad con los hosts, el Vcenter Server y los switches.
- Verificamos las VLAN creadas y reglas de acceso a internet.
- Finalmente, generamos y almacenamos un backups de la correcta configuración actual para su utilización en caso necesario.

4.2. Instalación y configuración del vCenter Server

Cuando el tamaño de una infraestructura virtual crece, la capacidad para gestionar la infraestructura desde un punto central comienza a ser muy importante [3]. En una infraestructura virtual con uno o dos ESXi el esfuerzo que hay que desempeñar para la administración de la misma no es muy reseñable. Sin embargo, cuando el número de host comienza a crecer, y con este el número de máquinas virtuales a gestionar, el esfuerzo en la gestión de la plataforma crece de forma exponencial. Estrictamente hablando, vCenter Server no es un elemento indispensable para el despliegue de una plataforma VMware vSphere ya que se pueden desplegar y arrancar máquinas virtuales sin un vCenter Server. Sin embargo, para utilizar las funcionalidades avanzadas de la suite de productos vSphere, vCenter Server debe ser licenciado, instalado y configurado adecuadamente.

Vcenter Server permite disponer de las ventajas de la arquitectura cliente-servidor en la arquitectura de los host ESXi y las máquinas virtuales que gestionan. El vCenter Server proporciona la gestión centralizada y monitorización de toda la plataforma virtual VMware vSphere 5,

incluyendo la implementación de reglas de rendimiento/negocio, scripting y correlaciones de eventos ante diferentes situaciones. Permite gestionar centralizadamente múltiples servidores VMware vSphere ESXi y máquinas virtuales. Una sola instancia de vCenter Server soporta un máximo de 1.000 hosts ESXi y 15.000 máquinas virtuales registradas (10.000 máquinas virtuales encendidas).

El vCenter Server añade funcionalidad en áreas tales como alta disponibilidad (VMware HA), actualización de componentes (Update Manager), conversiones de físico a virtual (VMware Converter) y migración en vivo de máquinas virtuales entre hosts ESXi (vMotion). Existen más funcionalidades dependiendo de la licencia adquirida como ya se ha explicado en apartados anteriores. Las principales características de VMware vCenter Standard son expuestas a continuación:

- Funcionalidades avanzadas: gestión de recursos para hosts ESXi y máquinas virtuales, programación de tareas, gestión de plantillas, registro de estadísticas, gestión de alarmas y eventos, aprovisionamiento de máquinas virtuales y configuración del host y las máquinas virtuales.
- Servidor de bases de datos, que da acceso a la base de datos del vCenter. almacena los datos de configuración persistentes y la información de rendimiento.
- Servicio de inventario, que permite a los administradores buscar en todo el inventario de objetos de varios VMware vCenter Server desde una sola ubicación.
- Clientes de VMware vSphere, que proporciona a los administradores una consola con gran cantidad de funciones que permite acceder a los hosts ESXi de forma independiente o a la gestión de la plataforma virtual completa mediante la conexión al VMware vCenter Server.
- API y .NET de VMware vCenter, permiten la integración entre vCenter Server y otras herramientas, y admiten complementos personalizados en VMware vSphere Client.
- vCenter Single Sign-On, que permite el acceso a todos los elementos de la plataforma mediante un único inicio de sesión, simplificando la administración.
- vCenter Orchestrator: simplifica y automatiza los principales procesos del vCenter Server.
- vCenter Server Linked Mode: ofrece una vista de inventario común que abarca varias instancias de vCenter Server.

Hay componentes, herramientas y utilidades adicionales al vCenter Server que pueden ser añadidos al servidor de vCenter cuando sean necesarios:

- Cliente Web VMware vSphere: permite la gestión de las funciones esenciales de vSphere desde cualquier navegador.

- VMware vSphere Update Manager: automatiza la gestión de parches y elimina la necesidad de hacer el seguimiento y la aplicación de parches de forma manual en los hosts y máquinas virtuales de vSphere.
- VMware VSphere Syslog conector y VMware vCenter ESXi Dump Collector: permite crear un centro común de almacenamiento y gestión de logs de los equipos de la infraestructura virtual.
- VMware Auto Deploy: simplifica el despliegue y la conformidad de los hosts mediante la creación de máquinas virtuales a partir de plantillas de configuración.
- VMware VSphere Authentication proxy: posibilidad de desplegar un proxy intermedio entre los hosts y nuestro dominio o Active Directory.
- Vcenter Host Agent Pre-Upgrade checker: permite comprobar si las características de un host son las adecuadas antes de actualizarlo a una versión de VMware VSphere ESXi superior.

La arquitectura de vCenter se basa en:

- Cliente VMware vSphere: el mismo cliente de vSphere que se utiliza para gestionar los hosts sirve también para conectarse al sistema vCenter Server.
- Dominio de Active Directory: la seguridad del sistema vCenter Server se puede integrar con la seguridad de Windows, aunque se puede utilizar vCenter Server sin que pertenezca a un dominio, como será nuestro caso.
- Hosts gestionados: vCenter Server permite gestionar tanto los hosts ESXi como las máquinas virtuales que se ejecutan en ellos.
- Base de datos de vCenter Server:

Los requisitos mínimos para la instalación de Vcenter Server 5 son expuestos a continuación [3]:

Requisitos Hardware (Versión Windows):

- Procesador: 2 CPUs 64-bit 2.0 GHz Intel o AMD x86.
- Memoria: 3 GB RAM mínimo.
- Disco: 3 GB de espacio libre.
- Red: Adaptador Ethernet (1 Gigabit altamente recomendado).

Requisitos Software:

- Windows XP Pro 64-bit, SP2 y SP3

- Windows Server 2003 64-bit Standard, Enterprise y DataCenter, SP1 y SP2
- Windows Server 2008 64-bit Standard, Enterprise y DataCenter, SP2
- Windows Server 2008 R2 64-bit

La cantidad de hardware que vCenter Server requiere está directamente relacionada con el número de hosts y máquinas virtuales que va a gestionar. Las mejores prácticas *de* VMware vSphere 5.0 [9] recomiendan un servidor con 2 CPUs y 4GB de RAM para soportar la gestión de hasta 50 ESXi hosts y 500 máquinas virtuales encendidas. En el caso de las grandes arquitecturas que despliegan cientos de ESXi, a parte de disponer de varios vCenter Server enlazados, utilizan servidores separados para la instalación del vCenter Server y la base de datos de gestión de este, en lo que se denomina servidor backend del vCenter Server. Esta arquitectura optimiza la gestión y la recuperación de desastres y continuidad de negocio del VMware vCenter Server.
En la arquitectura virtual a implantar en nuestro caso el vCenter Server residirá en un servidor físico cuyas características son mostradas en la siguiente tabla, cumpliendo con creces los requisitos mínimos de instalación del vCenter Server 5:

Nombre	Modelo	CPU	RAM(GB)	IP	Puertos de Red	Puertos FC	Sistema Operativo	Otras caracteristicas
vCenter Server	DELL PowerEdga R410 OEM	2 CPU Intel(R) Xeon(R) E5606 2.13 GHz Quadcore	24	192.168.0.150	2 Gigabit	2 Qlogic 8Gb FC Dual Port HBA	Windows Server 2008 Standard R2 SP1 64 bits	Fuente de alimentación redundada, 500 GB HDD, 3 años de soporte 24x7

Tabla 6: Características del servidor vCenter

Como puede verse en la tabla anterior, el servidor físico cumple con los requisitos mínimos y recomendados por VMware para la instalación del vCenter Server y la gestión de una arquitectura virtual de 6 ESXi y aproximadamente entre 40 y 50 máquinas virtuales encendidas.

Quizás el componente más importante en vCenter es su base de datos. vCenter Server 5 almacena todos los datos del inventario, pool de recursos, funciones de seguridad, datos de rendimiento, permisos y cuentas de usuario, estado de cada máquina virtual y configuración de cada servidor VMware vSphere ESXi, en una base de datos relacional. Las bases de datos soportadas por vCenter Server para Windows son las siguientes:

- Oracle 10g R2
- Oracle 11g R1 y R2
- IBM DB2 9.5 y 9.7
- Microsoft SQL Server Server 2005 SP3 (recomendado SP4)
- Microsoft SQL Server 2008 R2 Express (solo recomendable con hasta 6 hosts y 50 MV)
- Microsoft SQL Server 2008
- Microsoft SQL Server 2008 R2

Para el vCenter Server de la arquitectura virtual a desplegar, se utilizó una base de datos Microsoft SQL Server 2008 R2 SP1 Edición Express (versión 10.50.2500.0) mediante una instalación local en el mismo servidor físico. Al disponer de una arquitectura virtual pequeña, la versión Express gratuita del servidor de base de datos de Microsoft nos permitiría gestionar sin problemas la base de datos del vCenter Server de la empresa. Ya en el futuro a medio plazo, con la arquitectura virtual ya más madura y con la mayoría de las aplicaciones desplegadas, el crecimiento de la misma nos puede llevar a plantear una arquitectura con servidores independientes específicos para la instalación del vCenter Server y la base de datos del mismo con una versión de Microsoft SQL Server de pago.

En la versión VMware vSphere 5 se incluyó por primera vez la opción de instalar vCenter Server en Linux, utilizando la descarga de un *appliance virtual*, es decir, la descarga de una máquina virtual, específicamente diseñada por VMware, con sistema operativo Linux que viene con vCenter Server preinstalado. Esto tiene la ventaja del ahorro de costes al no tener que utilizar una licencia específica de Microsoft Windows Server para instalar el Vcenter Server. Sin embargo, el appliance cuenta con algunas limitaciones con respecto a la versión Windows que son descritas con detalle en [3]. Mi empresa decidió realizar la instalación en Windows, concretamente en Windows Server 2008 Standard R2, porque contaba con un mejor soporte, incluía más funcionalidades, una versión más estable, y la administración y uso era más ágil y fácil. Además, como detallaremos más adelante, el servidor físico donde se realiza la instalación del vCenter Server se iba a utilizar para otras funciones importantes que necesitaban el sistema operativo Microsoft Windows para desempeñarlas.

Cabe destacar que el vCenter supone un centro de gestión y administración de la infraestructura virtual, pero la interrupción de su funcionamiento no afectaría a los servicios desplegados desde la plataforma virtual al exterior/interior de la empresa, es decir, las máquinas virtuales seguirían funcionando sin problemas. Sin embargo, la interrupción del vCenter Server provoca que toda la funcionalidad que nos aporta (vMotion, update manager, creación de máquinas virtuales, gestión de los datastores, etc.) dejaría de estar disponible. Por este motivo, vCenter Server debe ser incluido en los planes de recuperación de desastres y continuidad de negocio. Lo que si permanecería tras la caída del Vcenter Server es el servicio de alta disponibilidad de vSphere, ya que este se gestiona a nivel de clúster de hosts aunque se administre a nivel de Vcenter.

Para la configuración/instalación del vCenter Server se utilizará el siguiente procedimiento [1][3][25]:

1. Instalación física del servidor: desempaquetamos y enracamos el servidor en el CPD. Lo conectamos a la corriente eléctrica y lo arrancamos.
2. Se realizan las conexiones del cableado de Fibra en las tarjetas HBAs y las conexiones del

cableado RJ45 en las interfaces ethernet según los esquemas que describen dicha conectividad y que se han diseñado en el capítulo 3.

3. Instalación del sistema operativo Windows Server 2008 Standard R2. Tras esto, realizamos la configuración inicial del mismo: creación de cuentas de usuarios para la administración segura del servidor y asignación de las IPs correspondiente a sus interfaces de red.
4. Instalación de Microsoft SQL Server 2008 R2.

   Para la instalación de Vcenter Server utilizaremos una base de datos local instalada en el mismo servidor físico. Por ello, realizaremos la instalación de motor de base de datos SQL Server 2008 R2 edición Express.
5. Creación de la base de datos y del propietario de la misma con todos los permisos sobre ella. Para ello, en este punto creamos la base de datos para el vCenter Server con el nombre *VIM_VCDB*. Como propietario de la base de datos, creamos el usuario *vpxuser*, que es el usuario que vCenter Server usa para conectar a la base de datos, y fijamos a este usuario como propietario de la base de datos *VIM_VCDB*.

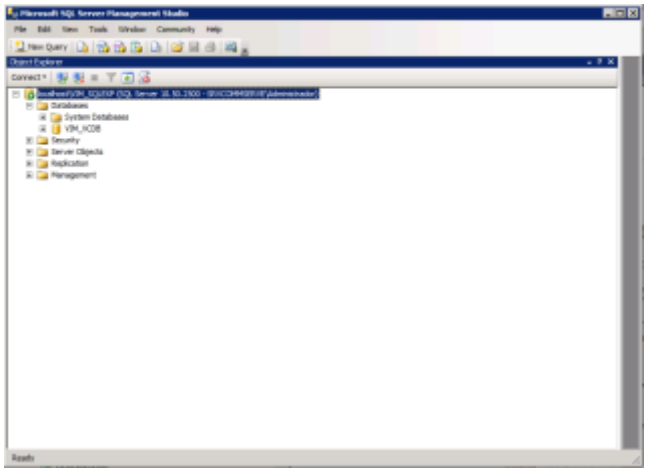


Figura16: Base de datos VIM_VCDB para Vcenter Server

6. Creación de un ODBC DSN* (*Open Database Conectivity Data Source Name*) de 64 bits. La instalación de vCenter Server 5 requiere la creación de un DSN y que la conectividad ODBC, que se crea antes de instalar el servidor de vCenter, sea de 64bits. Este ODBC se utiliza para conectar la base de datos con el vCenter y durante su creación elegimos la base de datos sobre la que conectaremos, *VIM_VCDB*, y el usuario utilizado para la autenticación con los permisos adecuados, *vpxuser*.

* Si la instalación de SQL Server no la incluye, es necesario descargar e instalar SQL Server 2008 R2 Native Client para configurar el ODBC DSN

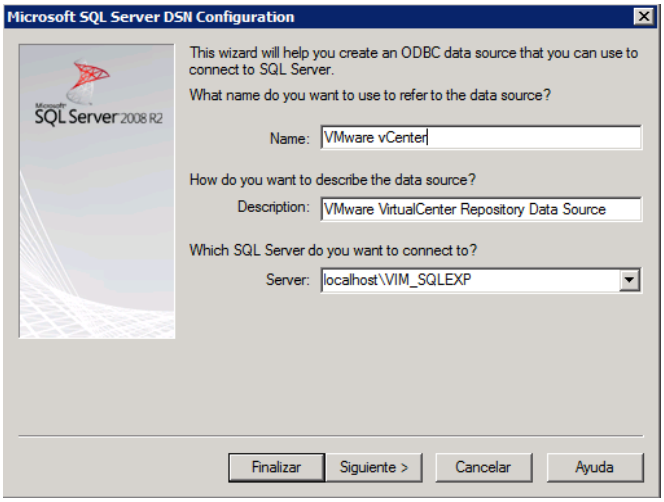


Figura17: DSN de 64 bits para Vcenter Server

7. Descarga de la última versión disponible de la suite de productos del VMware vCenter Server en el servidor donde vamos a realizar su instalación desde la web del fabricante VMware.
8. Instalación de los prerrequisitos Microsoft NET 3.5 SP1 y Windows Installer 4.5. A continuación, instalación del programa VMware Vcenter Server 5 a través del instalador del VMware vCenter:

Figura 18: Instalador VMware vCenter

Durante la instalación el *Wizard* para el vCenter Server nos pedirá que completemos:

- Nombre de usuario, organización y clave de licencia del producto que adquirimos en VMware para la versión Standard del VMware vCenter Server.
- Información de base de datos. Se indica la base de datos a utilizar, en nuestro caso SQL Server 2008 R2 SP1 Edición Express, indicando el DSN ODBC que creamos en los pasos anteriores.
- La información de la cuenta con las credenciales para autenticar contra vCenter Server.

- Directorio destino dentro del servidor físico donde se alojará el software: nombre de la carpeta predeterminada en la que se instalará el software de vCenter Server. Dejamos la opción por defecto.
- Indicamos que la instancia de Vcenter Server se instalará como independiente y no se unirá a un grupo Linked Mode.
- El FQDN para el vCenter Server, ya que no se puede utilizar la IP del servidor.
- Los puertos a utilizar por Vcenter Server. Utilizamos los puertos por defecto que indica el propio instalador, opción recomendada por VMware si es posible: 443 (HTTPS), 80 (HTTP), 902 (protocolo de *heartbeat* de VMware), 8080 (Web Service HTTP), 8443 (Web Service HTTPS), 60099 (notificación de cambio de servicio web), 389 (LDAP) y 636 (SSL).
- El tamaño aproximado que tendrá la arquitectura virtual que administrará la instancia de vCenter Server: Pequeña (menos de 100 hosts o 1000 máquinas virtuales).

9. El siguiente paso para poder comenzar a utilizar vCenter Server es instalar el cliente VMware vSphere. Este cliente puedes instalarlo en cualquier PC para acceder al vCenter Server y se puede descargar el paquete para su instalación desde cualquier host ESXi que tenga instalado el hipervisor VMware Vsphere, accediendo a él mediante el navegador: http://<nombre_esxi> o http://<ip_host_esxi>. Cabe resaltar que el cliente VMware vSphere permite también conectarse a cada host de forma individual para su gestión, con usuarios definidos de forma local en cada ESXi y, de este modo, gestionar las máquinas virtuales que se alojan en ese host.

   El cliente de VMware vSphere permite realizar la gestión y administración completa de la arquitectura virtual a través de la información y operaciones que nos permite el vCenter Server.
10. Instalación del cliente web VMware vSphere que nos permite acceder al Vcenter desde cualquier navegador. Se trata de una versión del cliente vSphere basada en Adobe Flex que se abre en un navegador y es completamente extensible e independiente de la plataforma.

Con este procedimiento ya dispondríamos de la instalación del Vcenter Server. El siguiente paso es acceder al Vcenter Server a través del cliente VMware vSphere. Tras acceder al menú principal, se navega hasta el apartado *Inventory* > *Host and Cluster* y se crea un nuevo *datacenter* que será donde se comenzará a crear y alojar todos los elementos de la arquitectura virtual. Para ello, se

utiliza la opción *Add Datacenter* mediante el botón derecho sobre el objeto de inventario vCenter Server.

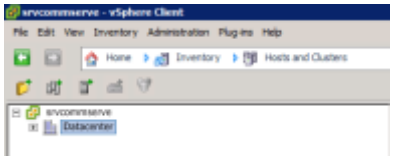


Figura 19: Creación del Datacenter de la infraestructura virtual

De este modo, a través del Vcenter Server ya podemos gestionar los servidores físicos que deben estar conectados en la misma subred que el Vcenter Server. A este servidor vCenter también se le presentarán las unidades de almacenamiento que también serán presentadas a los servidores ESXi desde la cabina y formateadas con el sistema de ficheros VMFS.

Además, en nuestro caso, utilizaremos el servidor físico donde se ha instalado el vCenter Server para otras tareas importantes dentro de la infraestructura virtual que son expuestas a continuación:

- Centro de gestión remota de switches Ethernet y Fiber Channel a través de las herramientas webs de administración de los dispositivos. Nos servirá para hacer cambios en la configuración, actualización de firmware y backups de las configuraciones.
- Centro de gestión remota de las cabinas de almacenamiento para cambios en la configuración, monitorización de la cabina, actualización de firmware y backups de las configuraciones.
- Servidor donde se instalará la herramienta de copias de seguridad profesional Commvault Simpana.
- Centro de datos para la monitorización de la arquitectura virtual.
- Centro de descarga de software (ejemplo distribuciones Linux) para instalar en las máquinas virtuales de la arquitectura virtual.

Por último, resaltaremos que VMware vCenter Server es la interfaz recomendada para asignar licencias a los hosts de VMware vSphere. Cuando VMware vCenter Server asigna una clave de licencia, esta se copia en el host y se guarda en formato persistente. En caso de que el host se desconecte de VMware vCenter Server, la clave de licencia sigue estando activa en el host por tiempo indefinido, incluso aunque se reinicie el host. Las claves de licencia de host solo pueden eliminarse o reemplazarse si un usuario realiza una operación deliberada con ese fin. Esto permite realizar una asignación de licencias centralizada sin punto único de fallo.

4.3. Instalación y configuración de los servidores físicos ESXi

En este apartado se describe toda la configuración de cada uno de los hosts ESXi que conforman la plataforma VMware de la arquitectura virtual. Los ESXi son los servidores donde se ejecuta el kernel que proporciona VMware, que permite la virtualización de máquinas y servidores virtuales. Para este propósito se dispone de 6 servidores: 3 servidores IBM System x3550 M3 y 3 servidores DELL R410 OEM. La tabla que se presenta a continuación muestra desglosadas las características de los servidores ESX implantados:

Nombre	Modelo	CPU	RAM(GB)	IP	Puertos de Red	Puertos FC	Version ESX
ESX1	IBM System x3550 M3	2 CPU Quadcore Intel Xeon E5606	24	192.168.0.151	6	2	ESXi 5 Update 1
ESX2	IBM System x3550 M3	2 CPU Quadcore Intel Xeon E5606	24	192.168.0.152	6	2	ESXi 5 Update 1
ESX3	IBM System x3550 M3	2 CPU Quadcore Intel Xeon E5606	24	192.168.0.153	6	2	ESXi 5 Update 1
ESX4	DELL R410 OEM	2 CPU Quadcore Intel Xeon E7330	24	192.168.0.154	2	2	ESXi 5 Update 1
ESX5	DELL R410 OEM	2 CPU Quadcore Intel Xeon E7330	24	192.168.0.155	2	2	ESXi 5 Update 1
ESX6	DELL R410 OEM	2 CPU Quadcore Intel Xeon E7330	24	192.168.0.156	2	2	ESXi 5 Update 1

Tabla 7: Características de los servidores ESX

La primera tarea a realizar es la instalación física de los servidores [26][27]: desempaquetamos y enracamos los seis servidores en el bastidor de nuestro CPD y los conectamos a la corriente eléctrica. Tras finalizar esta operación, hay que proceder a la instalación de la suite VMware vSphere en cada servidor. La versión instalada de kernel para los seis servidores es **VMware ESXi 5 Update 1.** Para la instalación del VMware ESXi 5 Update 1 realizamos el siguiente procedimiento [1][3][28]:

En primer lugar, descargamos VMware ESXi 5 Update 1 de la página de VMware y lo grabamos en un DVD. El hipervisor de VMware es gratuito por lo que se puede descargar directamente en formato ISO desde la web de VMware. Para la instalación utilizaremos una unidad lectora de DVD externa con conexión USB porque los servidores no disponen de una. Los requisitos mínimos para su instalación son:

- CPU de 64 bits de 2 cores (Intel-VT o AMD-V). Máximo 160 CPUs
- 2GB de Memoria RAM. Máximo 1 TB.
- 5.2GB de Disco Duro
- 1 Interfaz Ethernet Gb. El número máximo de tarjetas de 1 GB Ethernet por servidor es de 32.

A continuación para cada uno de los seis servidores a instalar realizamos el siguiente procedimiento para la instalación interactiva de VMware ESXi 5 Update 1:

1. Accedemos a la BIOS del servidor y creamos un RAID1 con los dos discos del sistema. En el caso de los servidores IBM utilizamos la herramienta del fabricante MegaRAID BIOS Config Utility Drives. En el caso de los servidores DELL, el RAID de los discos del sistema venía realizado de fábrica. De este modo, conseguimos redundancia a nivel de disco de sistema en cada servidor.

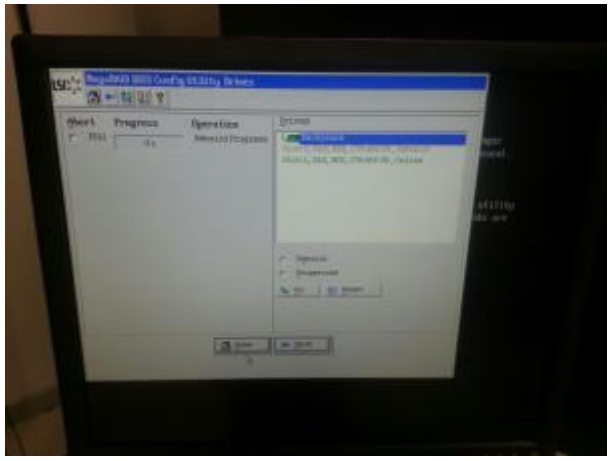


Figura 20: Realizando RAID con MegaRAID BIOS Config

2. Activamos en la BIOS de cada servidor la característica Intel-VT (Intel Virtualization technology) para permitirnos realizar la virtualización del servidor físico.
3. Activamos en la BIOS la opción de arranque desde la unidad lectora de DVD.
4. Insertamos el DVD que contiene el **ESXi 5 Update 1** y arrancamos el sistema con este boot-DVD.
5. Siguiendo el asistente de instalación de VMware realizamos la instalación del hipervisor en el disco del sistema de cada servidor utilizando el Wizard que proporciona VMware:
    - Seleccionamos el teclado español.
    - Seleccionamos el disco del local sistema, en RAID1 realizado anteriormente, para que se despliegue la instalación. Este disco no debe estar formateado con VMware vSphere VMFS:

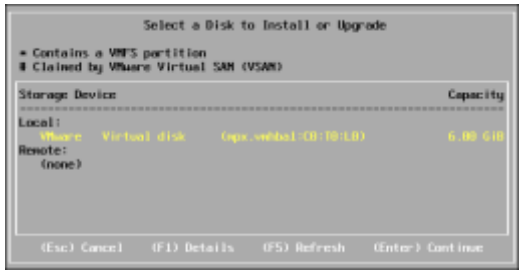


Figura 21: Seleccionamos el RAID1 para realizar la instalación

Para evitar cualquier tipo de confusión se recomienda no conectar las conexiones de fiber channel en las tarjetas HBAs del servidor para evitar realizar la instalación en otro disco que no sea el local del servidor, lo que podría provocar borrado de información.

- Fijamos la contraseña para el usuario root para el acceso al hipervisor ESXi.
- Realiza la comprobación de la compatibilidad del hardware del servidor y si no ha detectado ningún problema se completa la instalación en unos minutos. Los servidores cumplen los requisitos mínimos para la instalación y hemos habilitado el Intel-VT.
- Tras completar la instalación con éxito, el sistema se reinicia y ya se dispone del hipervisor en el servidor. La instalación te permite un período de funcionamiento de 60 días hasta que se licencien los hosts a través del Vcenter.

6. Una vez completada la instalación, se realiza la personalización de la configuración del mismo. Esto se realiza en la interfaz de usuario de la consola directa (DCUI) del servidor. Para ello:
   - Se fija el nombre de cada host.
   - Se seleccionan como activos los 2 adaptadores de red que vamos a utilizar en cada ESXi y que son los únicos que nos va a detectar.
   - Se fija como VLAN ID el 10, VLAN en la que se integrarán todos los ESXi y que servirá también como **red de gestión** VMware VSphere.
   - Se configura la IP fija de cada host según la información descrita en la tabla 7. Se utilizará la característica *Teaming* de VMware que permite disponer de 2 interfaces de red activas como si fueran una sola, consiguiendo redundancia a nivel Ethernet y utilizando la capacidad de las 2 interfaces de red, aunque solo direccionamos con una IP. Se fijan también los datos del Gateway y la máscara de red según la configuración de red.
   - Se configura el DNS primario y secundario. Como no se dispone de DNS a nivel empresarial, se fijan unos externos conocidos, que son los de la empresa que gestiona el registro de dominios de internet de la empresa.
7. Se realizan las conexiones del cableado fiber channel y red Ethernet en cada host según los esquemas que describen dicha conectividad y que se han diseñado en el capítulo 3.
8. Tras completar la configuración del host podemos comprobar la conectividad y gestionarlo a través del Vcenter Server. Por ello, añadimos cada host ESXi, en el que hemos realizado la

instalación del hipervisor de VMware, al *Datacenter* creado en el apartado anterior. Esto lo veremos en el apartado de creación del contenido de la plataforma VMware.

4.4. Instalación y configuración de la red SAN Fiber Channel

Toda la información de la plataforma de virtualización VMware se encuentra centralizada en la red de almacenamiento SAN, compuesta por una cabina de almacenamiento DS3524 de IBM, dos switches FC Express IBM System Storage SAN2 4B-4 y el cableado físico de fibra. Para conectarse a la SAN cada servidor host ESXi y el vCenter Server disponen de una tarjeta HBA de doble canal.

Desde la consola de administración de la SAN se podrán administrar y presentar los discos duros que queramos a los servidores que se estime oportuno. La ventaja de este sistema es que todos los discos quedan en la cabina y pueden ser presentados a cualquier servidor según las necesidades. De este modo, los servidores que forman el clúster de la arquitectura virtual pueden ver los mismos discos duros de la SAN, permitiendo disponer de redundancia y tolerancia a fallos a nivel de host y a nivel de máquina virtual. Si una máquina virtual cae, por error del sistema operativo o avería del hardware del host físico que la alberga, como dicha máquina virtual está en la SAN, esta puede volver a funcionar en otro servidor host con tarjeta HBA que accede también a la SAN sin pérdida de servicio. La característica de VMware vMotion es la que se encarga de levantar la máquina virtual en otro host disponible dentro del clúster de ESXi de VMware sin interrupción de servicio.

Con este sistema de almacenamiento, se consigue separar el almacenamiento de la plataforma del servidor que accede a él, lo que redunda en una mayor disponibilidad, tiempo reducido de respuesta a errores y alta tolerancia a fallos.

4.4.1 Instalación y configuración switches FC

En este apartado se va a explicar detalladamente el procedimiento de instalación y configuración de los dos switches Express IBM System Storage Brocade 249824E. Dicho procedimiento es descrito a continuación [29]:

1) Instalación física de los switches FC: desempaquetamos y enracamos los dos switches en el bastidor de nuestro CPD.
2) Conexión de los switches a la red eléctrica y encendido de los mismos.
3) Se realiza la configuración inicial de cada switch.

Para su inicialización y gestión, cada switch dispone de dos puertos RJ45, uno para conectividad Ethernet y otro para conectividad a través de un puerto serie de consola. En nuestro caso utilizamos el puerto Ethernet. Para la configuración inicial utilizamos el programa para la gestión y configuración de los switches que proporciona el fabricante *Brocade EZSwitchSetup* [30] y conectamos cada switch FC a configurar a la misma subred que el ordenador donde instalamos el software *EZSwitchSetup*, utilizando su puerto Ethernet y un cable RJ45. Para ello, se utilizó un switch Ethernet de 8 puertos independiente a los incluidos en la arquitectura virtual y destinado a la configuración inicial de este dispositivo. La IP por defecto del switch FC es 10.77.77.77 y para poder acceder a él colocamos una IP de esta misma subred en el ordenador desde el cual vamos a configurar el switch. Las credenciales de acceso por defecto son admin/password. En la configuración inicial se realizan las siguientes tareas:

- Asignamos una IP fija a cada switch.
- Accedemos al switch y configuramos los parámetros básicos.
    - Nombre del switch
    - Actualización de las credenciales de acceso/administración.

  En la siguiente tabla se muestra la configuración inicial de los switches:

Name	SW1	Name	SW2
Status	Healthy	Status	Healthy
Fabric OS version	v6.4.2a	Fabric OS version	v6.4.2a
Domain ID	1(0x1)	Domain ID	1(0x1)
WWN	10:00:00:05:33:f0:6d:67	WWN	10:00:00:05:33:f0:6d:67
Type	71.2	Type	71.2
Role	Principal	Role	Principal
Ethernet		**Ethernet**	
Ethernet IPv4	192.168.0.10	Ethernet IPv4	192.168.0.10
Ethernet IPv4 netmask	255.255.255.0	Ethernet IPv4 netmask	255.255.255.0
Ethernet IPv4 gateway	192.168.0.1	Ethernet IPv4 gateway	192.168.0.1
Ethernet IPv6	None	Ethernet IPv6	None
FC		**FC**	
IPFC IPv4	None	IPFC IPv4	None
IPFC IPv4 netmask	None	IPFC IPv4 netmask	None
Zone		**Zone**	
Effective configuration	cfg	Effective configuration	cfg
Other		**Other**	
Manufacturer serial number	ALJ2516H0M8	Manufacturer serial number	ALJ2516H0M8
Supplier serial number	10220VH	Supplier serial number	10220VH
License ID	10:00:00:05:33:f0:6d:67	License ID	10:00:00:05:33:f0:6d:67
RMD		**RMD**	
Type	002498	Type	002498
Model	24E	Model	24E
Tag	01ff	Tag	01ff
Sequence number	0000010220VH	Sequence number	0000010220VH
Insistent Domain ID Mode	Disabled	Insistent Domain ID Mode	Disabled
Manufacturer	IBM	Manufacturer	IBM
Manufacturer Plant	CA	Manufacturer Plant	CA

Tabla 8: Configuración inicial de los switches FC

Tras la configuración inicial podremos acceder a los switches para su configuración avanzada a través del programa *Brocade EZSwitchSetup*, TELNET, SSH o la herramienta de acceso web que proporciona el fabricante, denominada *Advanced Web Tools* [31].

4) Actualización del firmware de los switches FC a la última versión publicada por el fabricante. Las mejores prácticas recomiendan que ambos switches dispongan de la misma versión de firmware.

5) Conexión del cableado físico para conectar mediante cables de fibra las tarjetas duales HBA de los servidores físicos ESXi a cada switch FC, y las tarjetas HBA duales de cada controladora de las cabinas a cada switch FC. Se sigue en esquema de la figura 9.

6) Realización la configuración completa de los switches Fiber Channel.

Cabe resaltar que la alta disponibilidad de la red SAN a nivel de switch la logramos duplicando los caminos disponibles entre los dispositivos que van a acceder al almacenamiento y las controladoras que gestionan el acceso a ese almacenamiento. Esa duplicación de caminos lo conseguimos con los dos switches Fiber Channel, las dos controladoras de la cabina y los 2 canales de los que disponen las tarjetas HBA. Para la realización de la configuración completa se ha utilizado la herramienta de configuración *Advanced Web Tools*. La configuración completa de los switches se divide en los siguientes apartados:

a) Activación de las licencias

Para comenzar a utilizar los switches hay que activar la licencia de funcionamiento *Full Fabric Activation* en la página del fabricante. Los switches traen activados de fábrica 8 puertos, del puerto 1 al puerto 7, y, para la arquitectura SAN a implantar, se deben activar la licencia adquirida *8-Port-Activation* para activar los 8 puertos siguientes: del puerto 8 al puerto 15. De este modo, ya tenemos puertos suficientes para conectar en cada switch los cables de fibra procedentes de las HBAs de los seis ESXi, el servidor que actúa como vCenter Server y las dos controladoras de la cabina. La activación de las licencias se realiza a través de la web de IBM utilizando el *World Wide Name* (WWN) de cada switch FC y la clave de activación adquirida en IBM. Tras esto, IBM envía las licencias que son añadidas a los dispositivos a través de la herramienta *Advanced Web Tool*. En la siguiente figura podemos ver una imagen, extraída de la herramienta *Advanced Web Tool*, de la parte frontal del switch FC que se está configurando:

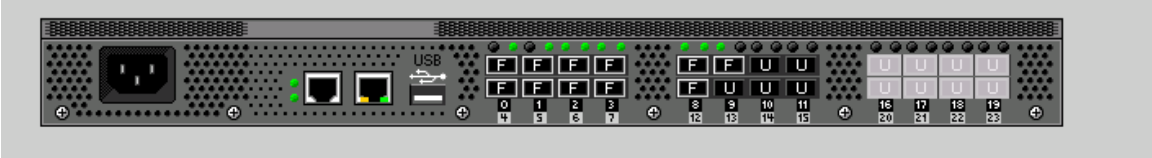


Figura 22: Parte frontal switch FC AT8000GS/48

b) Configuración de alias y zoning en los switches FC.

El objetivo perseguido en la red SAN es que cada servidor ESXi únicamente pueda comunicarse por fiber channel con su almacenamiento, de manera que no haya forma de que un servidor perciba la existencia de otro. Para conseguir esto se utiliza lo que se denomina como *zoning*. Los conceptos importantes a definir dentro del *zoning* son:

- Alias: es un nombre lógico que se establece a un dispositivo físico. Este dispositivo puede ser un puerto del switch (zonificación por hardware), o un WWN (zonificación por software), dentro de la SAN. Según el tipo de dispositivo, puerto o WWN, declarado en los alias se establece si la configuración global de las zonas se establece por puerto o WWN. Los alias son los nombres amigables que damos a los WWN para que sean fáciles de identificar y permiten identificar de forma más sencilla los elementos a la hora de hacer el zoning que si se hace por WWN o puerto.
- Zona*:* elemento que indica qué equipos pueden comunicarse entre sí. Una zona puede contener, un WWN, un alias, o un puerto Físico. Una zona es la relación entre dos o más dispositivos que permite que estos tengan comunicación a través del switch. Se creará una zona por cada grupo de dos dispositivos que deberán tener visibilidad en la SAN. Se asocian zonas a los WWN definidos, en grupos de 2, definiendo los caminos de comunicación fiber channel.
- zoneset*:* un zoneset es un conjunto de zonas. En un switch pueden existir varios zonesets definidos, pero únicamente puede haber uno activo.
- zoneset activo (o efectivo)*:* es el zoneset que está activo y es el mismo para todos los switches que componen el denominado switched fabric, topología de interconexión en la red SAN en la que los nodos interconectan entre sí a través de los switches como se muestra en la figura 9. Se corresponde con el archivo de configuración que contiene todas aquellas zonas que se han configurado como activas

Las ventajas de utilizar zoning son expuestas a continuación:

- Reduce el número de caminos entre un host y una LUN

- Mantiene los caminos primario y secundario en diferentes zonas.
- Mejora la seguridad al limitar los accesos entre nodos.
- Incrementa la fiabilidad al aislar los problemas.

b.1) Configuración de alias.

En nuestro caso, se van a definir los alias por zonificación por software a través de WWN. Por ello, se creará un alias en la configuración de zonas por cada nuevo dispositivo conectado a la SAN utilizando su WWN. A continuación, se muestra una tabla con los alias creados para cada tarjeta HBA en cada uno de los dos switches FC:

Alias	WWN
DS3524_SPA0	20:38:00:80:e5:2e:1b:4a
DS3524_SPB0	20:39:00:80:e5:2e:1b:4a
VCENTER_HBA0	21:00:00:24:ff:35:c7:32
ESX1_HBA0	21:00:00:24:ff:35:c7:2b
ESX2_HBA0	21:00:00:24:ff:35:c7:5b
ESX3_HBA0	21:00:00:24:ff:35:c7:2d
ESX4_HBA0	21:00:00:24:ff:35:c7:62
ESX5_HBA0	21:00:00:24:ff:35:c7:02
ESX6_HBA0	21:00:00:24:ff:35:c6:fe

Tabla 9: Alias switch 1

Alias	WWN
DS3524_SPA1	20:48:00:80:e5:2e:1b:4a
DS3524_SPB1	20:49:00:80:e5:2e:1b:4a
VCENTER_HBA1	21:00:00:24:ff:35:c7:33
ESX1_HBA1	21:00:00:24:ff:35:c7:2ª
ESX2_HBA1	21:00:00:24:ff:35:c7:5ª
ESX3_HBA1	21:00:00:24:ff:35:c7:2c
ESX4_HBA1	21:00:00:24:ff:35:c7:63
ESX5_HBA1	21:00:00:24:ff:35:c7:03
ESX6_HBA1	21:00:00:24:ff:35:c6:ff

Tabla 10: Alias switch 2

Para crear los alias en cada switch se accede a la herramienta *Advanced Web Tool* y en el apartado "*Zone Admin*", destinado a la definición de los alias y el zoning del switch FC, se definen los alias siguiendo las tablas anteriores. El switch detectará automáticamente los WWN de los dispositivos que tiene conectados a sus puertos. La configuración también puede realizarse accediendo por SSH a cada switch a través de la línea de comandos*.

b.2) Configuración del *zoning*.

Antes de realizar el zoning completo entre todos los elementos de la arquitectura SAN, es necesario que todos los elementos estén disponibles. Por ello, en este punto la cabina de almacenamiento DS3524 debe estar disponible y con los puertos de fibra debidamente configurados y conectados a los

* Comandos útiles utilizados: *cfgshow, cfgactvshow, alishow, zoneshow*

switches de fibra. Por ello, aunque el procedimiento de instalación y configuración de la cabina se ve en el apartado siguiente, su instalación inicial se realiza en paralelo con los switches fiber channel para tenerla disponible justo antes de la configuración del zoning.

Tras tener disponible todos los elementos de la red SAN, se procede a la configuración del zoning para que todos los elementos que componen la red sean visibles y accesibles entre sí. Para ello accedemos al switch a través de la herramienta *Advanced Web Tools* y realizamos la configuración en el apartado *Zone Admin*. En esta ventana podemos ver los alias, el zoneset y el zoneset activo. A continuación, se muestra una tabla con las zonas que serán creadas en los switches:

Alias	Zona	Alias
DS3524_SPA_HBA0	DS3524_SPA_HBA0_VCENTER_HBA0	VCENTER_HBA0
DS3524_SPA_HBA0	DS3524_SPA_HBA0_ESX1_HBA0	ESX1_HBA0
DS3524_SPA_HBA0	DS3524_SPA_HBA0_ESX2_HBA0	ESX2_HBA0
DS3524_SPA_HBA0	DS3524_SPA_HBA0_ESX3_HBA0	ESX3_HBA0
DS3524_SPA_HBA0	DS3524_SPA_HBA0_ESX4_HBA0	ESX4_HBA0
DS3524_SPA_HBA0	DS3524_SPA_HBA0_ESX5_HBA0	ESX5_HBA0
DS3524_SPA_HBA0	DS3524_SPA_HBA0_ESX6_HBA0	ESX6_HBA0
DS3524_SPB_HBA0	DS3524_SPB_HBA0_VCENTER_HBA0	VCENTER_HBA0
DS3524_SPB_HBA0	DS3524_SPB_HBA0_ESX1_HBA0	ESX1_HBA0
DS3524_SPB_HBA0	DS3524_SPB_HBA0_ESX2_HBA0	ESX2_HBA0
DS3524_SPB_HBA0	DS3524_SPB_HBA0_ESX3_HBA0	ESX3_HBA0
DS3524_SPB_HBA0	DS3524_SPB_HBA0_ESX4_HBA0	ESX4_HBA0
DS3524_SPB_HBA0	DS3524_SPB_HBA0_ESX5_HBA0	ESX5_HBA0
DS3524_SPB_HBA0	DS3524_SPB_HBA0_ESX6_HBA0	ESX6_HBA0
VCENTER_HBA0	VCENTER_HBA0_ESX1_HBA0	ESX1_HBA0
VCENTER_HBA0	VCENTER_HBA0_ESX2_HBA0	ESX2_HBA0
VCENTER_HBA0	VCENTER_HBA0_ESX3_HBA0	ESX3_HBA0
VCENTER_HBA0	VCENTER_HBA0_ESX4_HBA0	ESX4_HBA0
VCENTER_HBA0	VCENTER_HBA0_ESX5_HBA0	ESX5_HBA0
VCENTER_HBA0	VCENTER_HBA0_ESX6_HBA0	ESX6_HBA0

Tabla 11: Zoning switch 1

Alias	Zona	Alias
DS3524_SPA_HBA1	DS3524_SPA_HBA1_VCENTER_HBA1	VCENTER_HBA1
DS3524_SPA_HBA1	DS3524_SPA_HBA1_ESX1_HBA1	ESX1_HBA1
DS3524_SPA_HBA1	DS3524_SPA_HBA1_ESX2_HBA1	ESX2_HBA1
DS3524_SPA_HBA1	DS3524_SPA_HBA1_ESX3_HBA1	ESX3_HBA1
DS3524_SPA_HBA1	DS3524_SPA_HBA1_ESX4_HBA1	ESX4_HBA1
DS3524_SPA_HBA1	DS3524_SPA_HBA1_ESX5_HBA1	ESX5_HBA1
DS3524_SPA_HBA1	DS3524_SPA_HBA1_ESX6_HBA1	ESX6_HBA1
DS3524_SPA_HBA1	DS3524_SPB_HBA1_VCENTER_HBA1	VCENTER_HBA1
DS3524_SPA_HBA1	DS3524_SPB_HBA1_ESX1_HBA1	ESX1_HBA1
DS3524_SPA_HBA1	DS3524_SPB_HBA1_ESX2_HBA1	ESX2_HBA1
DS3524_SPA_HBA1	DS3524_SPB_HBA1_ESX3_HBA1	ESX3_HBA1
DS3524_SPA_HBA1	DS3524_SPB_HBA1_ESX4_HBA1	ESX4_HBA1
DS3524_SPA_HBA1	DS3524_SPB_HBA1_ESX5_HBA1	ESX5_HBA1
DS3524_SPA_HBA1	DS3524_SPB_HBA1_ESX6_HBA1	ESX6_HBA1
VCENTER_HBA1	VCENTER_HBA1_ESX1_HBA1	ESX1_HBA1
VCENTER_HBA1	VCENTER_HBA1_ESX2_HBA1	ESX2_HBA1
VCENTER_HBA1	VCENTER_HBA1_ESX3_HBA1	ESX3_HBA1
VCENTER_HBA1	VCENTER_HBA1_ESX4_HBA1	ESX4_HBA1
VCENTER_HBA1	VCENTER_HBA1_ESX5_HBA1	ESX5_HBA1
VCENTER_HBA1	VCENTER_HBA1_ESX6_HBA1	ESX6_HBA1

Tabla 12: Zoning switch 2

Las *mejores prácticas* del fabricante para tener una SAN bien estructurada [32] recomiendan crear una zona en cada switch por cada servidor de la red de almacenamiento y cada controladora de la cabina. En este caso tenemos 6 servidores ESXi por lo que generaremos 12 zonas en cada Switch de Fibra. Del mismo modo crearemos dos zonas por cada switch para la conexión entre el vCenter y las controladoras de la cabina. Por último, se deben definir las zonas que conectan el vCenter Server con cada uno de los servidores físicos, que serían 6 por cada switch. El vCenter se incluye también en la red SAN porque será el encargado de realizar las copias de seguridad y de asignar a las máquinas virtuales la LUN donde se almacenarán los archivos y datos de esta en la cabina.

Una vez configuradas todas las zonas observaremos que están disponibles en el apartado *Zone Config*, como se muestra en la siguiente figura para ambos switches FC:

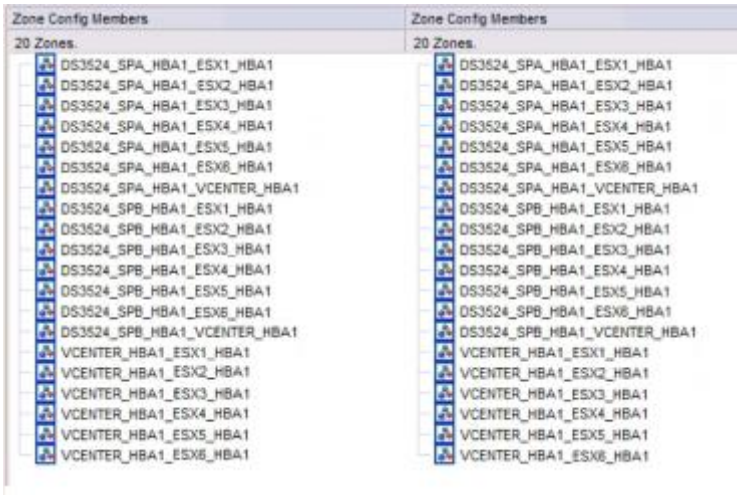


Tabla 13: Zoning completo

La misma configuración se debe llevar a cabo en ambos switches de Fibra donde estarán conectados los puertos redundantes tanto de las controladoras de la cabina como de las HBAs de los servidores.

En resumen, primero se realiza la interconexión física, pinchando físicamente el Fiber Channel y luego se conectan lógicamente mediante el zoning. Primero se hace desde el lado de los switches, estableciendo el zoning entre los ESX y la cabina, y luego nos conectamos a la cabina y vemos que se ven los ESXi.

7) Verificación de la configuración.

Para finalizar la configuración verificamos que la configuración del switch es la deseada. Para ello verificamos el correcto funcionamiento de los siguientes parámetros:

- La velocidad de los puertos.
- La conectividad con los hosts y la cabina de almacenamiento.

- Verificamos la configuración general de los switches.
- Verificamos la conectividad con los hosts, el vCenter y las cabinas.
- Finalmente, generamos y almacenamos backups de la correcta configuración actual para su utilización en caso de ser necesaria una restauración.

4.4.2. Instalación y configuración de la cabina IBM

En este apartado se va a describir el procedimiento seguido para la instalación y configuración de la cabina DS3524 de IBM [19][33][34]:

1. Preinstalación física de la cabina y primera puesta en marcha:
   - Desempaquetamos y enracamos la cabina en el bastidor del CPD.
   - Se realiza la inserción de los discos duros en las bandejas o unidades de disco de las cabinas. En total la cabina dispone de 24 discos de 1 TB.
   - Conectamos las cabinas a la corriente eléctrica y realizamos la primera puesta en marcha.
2. Se realizan las conexiones del cableado de Fibra y las interfaces Ethernet en cada una de las 2 controladoras de cada cabina según el esquema que describe dicha conectividad y que se han diseñado en apartados anteriores. En el caso de las conexiones de Fibra, conectamos los transceptores ópticos SFP (*small form-factor pluggable*) en cada tarjeta HBA de cada controladora. En la siguiente figura se muestra la información necesaria para la realización de estas operaciones:

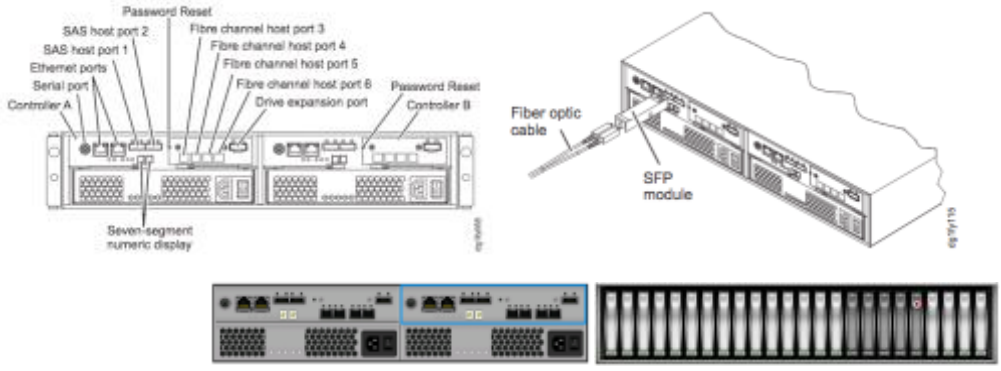


Figura 23: Cabina DS3524 (tomada de [30])

La longitud máxima del cableado de Fibra que acepta la cabina IBM DS3524 para la velocidad de 8Gbps es de 50 metros para cables de fibra multimodo 50/125 y de 35 metros para 62.5/125. En nuestro caso utilizaremos cableado de fibra 62.5/125 de 5m con conector LC-LC destinados a conexiones con alta densidad de datos y cumplimos este requisito sin

ningún problema.

3. Realizamos la configuración inicial de la cabina [30].

- Configuración del sistema de almacenamiento de la SAN. La administración de la cabina de almacenamiento IBM, que se conoce como *Storage Subsystem*, puede realizarse de dos formas:
  - Administración *Out-of-band*: Gestiona el sistema de almacenamiento a través de un servidor conectado a las interfaces Ethernet de las controladoras de la cabina.
  - Administración *In-band*: Gestiona el sistema de almacenamiento a través de un servidor conectado a la SAN mediante las conexiones de Fibra a través de las tarjetas HBA entre la cabina y el servidor.

  En nuestro caso utilizaremos la gestión *In-band* para la administración de la cabina porque se adapta mejor a nuestra infraestructura y como servidor de gestión se utilizará el servidor físico donde está instalado el vCenter Server. Además de la gestión *In band*, proporcionaremos a cada controladora de la cabina unas IPs fijas no para su gestión sino para su monitorización, ya que nos permitirá detectar si dichas controladoras están disponibles y, en consecuencia, si la cabina que las contiene también lo está. En la siguiente figura puede visualizarse la configuración realizada en la cabina principal:

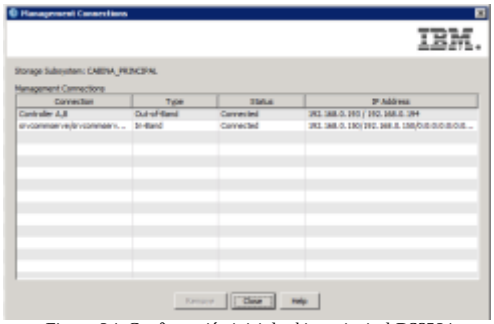


Figura 24: Configuración inicial cabina principal DS3524

  Como puede verse, utilizamos el vCenter Server (192.168.0.150) para gestionar directamente el sistema de almacenamiento, con conexión In-Band, y las IPs fijas de sus controladoras para monitorización de la misma (192.168.0.193/194), en conexión Out-of-Band para su monitorización.

- Instalación y configuración del sistema de almacenamiento. Antes de la configuración del sistema de almacenamiento, debemos asegurarnos de que las HBA están instaladas correctamente y actualizadas con el último firmware publicado por el fabricante. Lo mismo se

realiza para los drivers de los discos de la cabina. En nuestro caso, tanto las HBA como los discos disponen de la última versión del firmware y no es necesaria su actualización. En la siguiente figura se muestra el esquema SAN utilizado en la instalación siguiendo la documentación del fabricante:

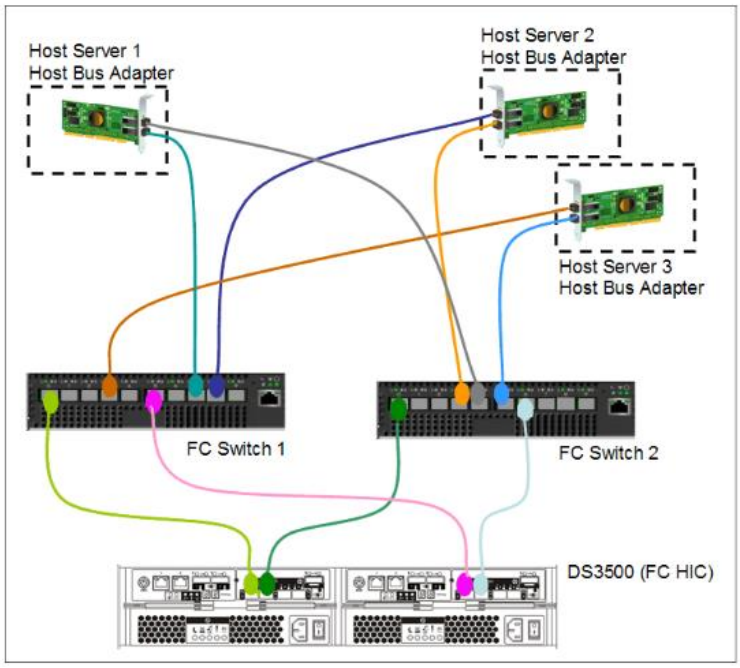


Figura 25: Configuración SAN Fiber Channel con canal dual (tomada de [30])

4. Realizamos la configuración avanzada de la cabina. En este apartado realizaremos la configuración del almacenamiento, configuración de los grupos de discos y RAIDs, inserción de las licencias, actualización del firmware y la configuración avanzada del sistema de la cabina.

Para la configuración avanzada de la cabina vamos a utilizar el software propietario que ofrece IBM para esta finalidad que se denomina DS Storage Manager. El propio fabricante entrega con el hardware de la cabina un dvd con la versión del programa que soporta el firmware de la cabina y podemos descargar versiones posteriores accediendo a la cuenta de cliente en la web de IBM. En nuestro caso instalamos la versión:

IBM System Storage DS Storage Manager (Enterprise Management) version 10.86.0G05.0028 for Microsoft Windows 64-bit editions

A continuación, realizamos la instalación del DS Storage Manager en el servidor Vcenter Server [35], que tiene conexión directa con la SAN y la cabina a través de su HBA de doble canal, utilizando el DVD proporcionado por el fabricante. La primera vez que accedemos, nos permitirá seleccionar la búsqueda de la cabina de forma automática utilizando la gestión *In-band*. También

permite realizar la búsqueda de la cabina de forma manual a través de la IP (gestión *Out-of-band*). Las IPs por defecto de las controladoras de cada cabina son:

Controladora A	Puerto 1	192.168.128.101
	Puerto 2	192.168.128.101
Controladora B	Puerto 1	192.168.128.102
	Puerto 2	192.168.128.102

Tabla 14: IPs por defecto de las controladoras

En nuestro caso marcaremos "Automatic" para que la descubra de forma automática y se iniciará el proceso de descubrimiento automático. La siguiente tabla muestra las IPs de funcionamiento en producción de las cabinas:

Controladora A	Puerto 1	192.168.128.193
	Puerto 2	192.168.128.194
Controladora B	Puerto 1	192.168.128.195
	Puerto 2	192.168.128.196

Tabla 15: IPs en producción de las controladoras

Tras esto ya podremos administrar nuestra SAN, desde la pestaña "Devices", haciendo doble click sobre la cabina que queramos administrar.

Figura 26: Configuración del almacenamiento a través del DS Storage Manager

Desde este punto podremos administrar y configurar de forma centralizada todas las características de la cabina. Para ello se realiza [34][35]:

- La inserción y configuración de las licencias de la cabina de almacenamiento.
  En este apartado cargamos la licencia de la cabina que nos ha proporcionado el fabricante IBM para disponer del soporte y de las características adicionales incluidas en la licencia. Para ello se utiliza la opción del DS Storage Manager *Manage Premium Feature*.
- Actualización de los drivers y firmware de las controladoras y elementos de la cabina a la última versión. Antes de la configuración avanzada de la cabina, se debe comprobar y actualizar los drivers y firmware de los siguientes elementos de la cabina y deben ser actualizados en el orden en el que se indica a continuación:

- Drive enclosure*: Versión del firmware ESM
- DS3524 Storage Server: Versión del firmware y versión NVSRAM.
- Hard Disk Driver: Versión del firmware.

Para la actualización de los diferentes firmware y driver se utiliza la opción *Update* del DS Storage Manager.

- Creamos la estructura lógica del almacenamiento. Para crear los arrays se utiliza el apartado *Storage* del software de administración de la cabina. Para el dimensionamiento de la plataforma virtual, se ha realizado la siguiente configuración a nivel físico y lógico en la cabina de almacenamiento IBM DS3524:
  - Creamos los Arrays. Disponemos de 24 discos, los cuales se van a agrupar en grupos o matrices de discos proporcionando mayor disponibilidad, resistencia y facilidad de administración. Los arrays configurados son mostrados en la siguiente tabla:

Nombre	RAID	Discos	Capacidad neta (GB)
Array 1	5	1,2,3,4,5	3,724
Array 2	5	6,7,8,9,10	3,724
Array 3	5	11,12,13,14,15	3,724
Array 4	5	21,22,23,24	2,793

Tabla 16: Arrays creados

El disco situado en la posición 20 de la cabina es un disco *Hotspare* global que permitirá reemplazar cualquier error en un disco averiado entrando en funcionamiento en el RAID determinado que contenga el disco con el error. El fabricante recomienda un disco *hotspare* por cada 18-20 discos del sistema y que el disco *hotspare* sea del mismo tipo y capacidad que el resto de discos. Los discos 16, 17, 18 y 19 conforman un espacio libre en cabina para futuras necesidades de 3,724 GB de espacio bruto.

El motivo de elegir RAID 5 ha sido el compromiso que se consigue entre redundancia y velocidad. RAID 5 es óptimo para entornos multiusuarios, como bases de datos o almacenamiento de sistemas de ficheros donde el tamaño de las operaciones E/S es considerable y hay una alta proporción de actividad de lectura. Es bueno para lecturas, operaciones concurrentes y operaciones aleatorias de E/S. Cuando más discos contengan los RAID 5 mejores prestaciones tendrán las transacciones de datos, pero se verá afectado el aprovechamiento de la capacidad. Sin embargo, con el fin de conseguir un compromiso entre

* Un enclosure de discos proporciona el suministro de energía necesario para que los discos funcionen y una o varias interfaces de conexión que permiten al host acceder a los discos contenidos en él. Además, traduce la información que recibe a través de la interfaz externa al formato nativo de los discos duros que aloja y viceversa.

prestaciones, capacidad y seguridad (el error en dos discos supondría pérdida de datos) se decidió realizar dos arrays de 5 discos y otro de 4 discos.

Con la difusión de los arrays de forma homogénea entre las dos controladoras conseguimos un mejor equilibrio de carga de trabajo. Sin embargo, cuando se asignan LUN a los hosts es importante tener en cuenta que la cabina da prioridad a una de las controladoras que toma en propiedad las comunicaciones con esa LUN, lo cual quiere decir que cada LUN es propiedad de una de las controladoras. Por esto, es importante asegurarse el correcto balanceo del tráfico entre las dos controladoras de cada cabina, lo cual es un principio fundamental para el correcto funcionamiento del sistema de almacenamiento. Para el correcto balanceo se realizaron las siguientes tareas:

- Asignar unidades lógicas a través de ambas controladoras para equilibrar la utilización del controlador.
- Utilizar el método manual de la creación de unidades lógicas, lo que permite una mayor flexibilidad para las opciones de configuración.
- Evitar la mezcla de tipos de carga de trabajo (nivel de transacción y nivel de rendimiento) en el mismo array de discos.
- Dejar siempre una pequeña cantidad de espacio libre en el array una vez creada las unidades lógicas para permitir ajustes futuros.

    - Creamos las unidades lógicas en la SAN (*Logical Drive*) en cada array. Estas unidades lógicas serán las LUN que se presentarán a los ESXi. Las unidades de almacenamiento han sido creadas con las siguientes características:

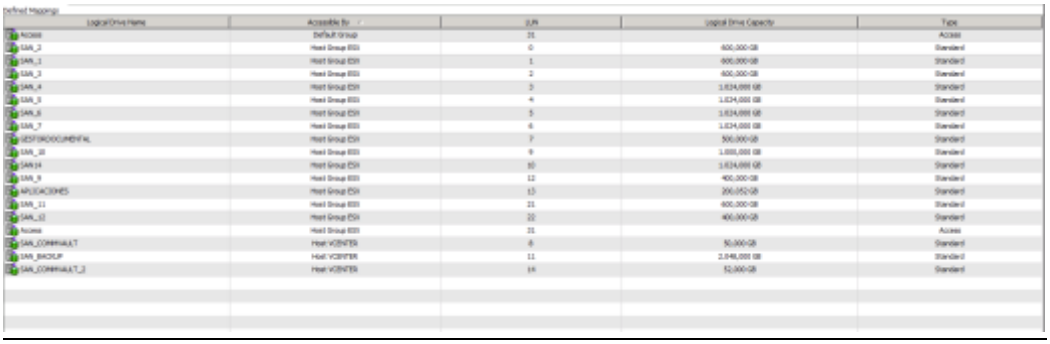


Tabla 17: Información LUN creadas

La figura anterior muestra las LUN creadas para albergar las máquinas virtuales que corren en los host ESXi. También existen otras LUN específicas que se han creado para un determinado servicio y que son solo accesibles por un determinado host. Ejemplo, una LUN denominada

SAN_COMMVAULT que se utiliza en exclusividad en el vCenter Server para las operaciones de backup y que solo es accesible desde este servidor. La LUN 31 denominada *Access*, es la LUN utilizada, en la configuración *In-band*, para la gestión cada host y siempre debe existir si se utiliza esta configuración.

Según esto, ha sido necesaria la creación de unidades de almacenamiento (LUN) en la nueva cabina IBM para presentarla a los servidores ESXi con el propósito de albergar los discos de las nuevas máquinas virtuales, los ficheros de configuración, snapshots y los ficheros de Log. Toda esa información es respaldada por el kernel de ESX, utilizando el sistema de ficheros VMFS versión 5 y tamaño de bloque 1 MB. Las LUN han sido presentadas en modo W/R (escritura/lectura) a todos los ESX, para que puedan acceder concurrentemente a ellas. Todo debe estar formateado siempre a VMFS (Virtual Machine File System) en los LUN de la cabina.

- Definir los hosts como miembros de la SAN.

En este apartado se identifican como miembros de la SAN los seis host ESX y el Vcenter Server. Las tarjetas HBA de fibra permiten a los hosts acceder a las LUN compartidas a través de la SAN. Para identificarlos y añadirlos utilizamos la opción de *Host Mapping*. A través de esta opción se pueden definir un nuevo Host en la SAN o un grupo de Host. En nuestro caso hemos identificado de forma individual cada uno de los ESX presentes en la SAN y el Vcenter Server. Luego se ha creado un grupo de hosts denominado *Host Group ESX* que incluye los ESX que componen el clúster de host VMWARE de la arquitectura virtual.

Host Port Identifier	Interface Type	Alias / User Label	Associated With Host
21:00:00:24:ff:35:c7:32	FC	VCENTER_HBA0	VCENTER
21:00:00:24:ff:35:c7:5b	FC	ESX2_HBA1	ESX2
21:00:00:24:ff:35:c7:2d	FC	ESX3_HBA0	ESX3
21:00:00:24:ff:35:c7:2b	FC	ESX1 HBA0	ESX1
21:00:00:24:ff:35:c7:33	FC	VCENTER_HBA1	VCENTER
21:00:00:24:ff:35:c7:5a	FC	ESX2_HBA0	ESX2
21:00:00:24:ff:35:c7:2a	FC	ESX1_HBA1	ESX1
21:00:00:24:ff:35:c7:2c	FC	ESX3_HBA1	ESX3
21:00:00:24:ff:35:c7:63	FC	ESX4_HBA1	ESX4
21:00:00:24:ff:35:c7:62	FC	ESX4_HBA0	ESX4
21:00:00:24:ff:35:c7:03	FC	ESX5_HBA1	ESX5
21:00:00:24:ff:35:c7:02	FC	ESX5_HBA0	ESX5
21:00:00:24:ff:35:c6:ff	FC	ESX6_HBA1	ESX6
21:00:00:24:ff:35:c6:fe	FC	ESX6_HBA0	ESX6

Tabla 18: Identificación de los hosts de la SAN

- Asignar unidades lógicas de la SAN a host de la red

A través de la opción *LUN Mapping* del *DS Storage Manager* se realiza la asignación de las distintas LUN creadas a los distintos host ESXi que forman el clúster y al Vcenter Server. Esta asignación puede verse en la tabla 12. En nuestro caso, para favorecer el vMotion y la alta disponibilidad permitimos de forma general el acceso de los servidores a todas las LUN y luego restringiremos el acceso a determinadas LUN solo a determinados host ESXi o al Vcenter Server dependiendo de que sea una LUN para una aplicación determinada o exclusiva de backups como es el caso de Vcenter Server.

Si bien permitimos el acceso de todos los ESXi de forma general a las LUN, luego a nivel funcional para una situación normal configuraremos las máquinas virtuales para que una determinada LUN sea accedida únicamente por un solo ESXi, lo cual aumentará el rendimiento, no sobrelimitará los accesos y permitirá que las HBAs que accedan a la misma LUN sean del mismo fabricante.
Los valores máximos para una SAN con Fiber Channel bajo vSphere VMware 5, y que se deben tener en cuenta en la configuración, son mostrados a continuación:

- 256 LUN por servidor.
- 64 TB por LUN.
- 255 LUN ID.
- 32 paths por LUN.
- 1024 paths por servidor.
- 8 HBAs de cualquier tipo.
- 16 puertos HBA.
- 256 targets por HBA.

En la siguiente imagen se muestra el resumen de la configuración realizada en la CABINA PRINCIPAL IBM DS3524:

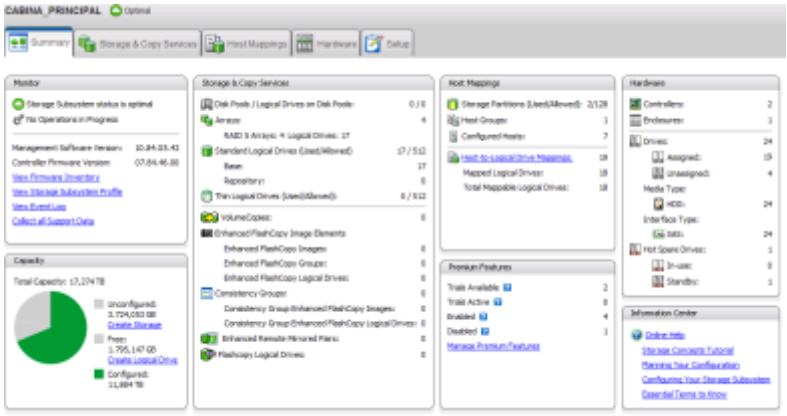


Figura 27: Configuración final del almacenamiento en la cabina principal IBM DS3524

Otras configuraciones avanzadas disponibles en la cabina:

- Seguridad: Cifrado de discos y establecimiento de password de acceso.
- Características Premium: que ya han sido definidas en apartados anteriores. En nuestro caso solo vamos a utilizar el *Enhanced Remote Mirroring*. Los servicios incluidos son:
  - Enhanced Remote Mirroring.
  - Drive Slot Limit.
  - Enhanced Flash Copy.
  - Flashcopy Logical Drive
- Monitorización del sistema con informes *Health* y de control de eventos y logs
- Hardware: configuración, control y monitorización de los elementos físicos de la cabina: Temperatura, discos, controladoras, HBAs, ventiladores, fuentes de alimentación, relojes de las controladoras, etc.

5. Seguir las mejores prácticas [34] que recomienda el fabricante en su documentación para el buen mantenimiento y configuración de las cabinas.
6. Banco de pruebas de funcionamiento. Esto lo verificaremos realmente cuando se añadan los datastores a cada Host ESXi dentro de la configuración de la plataforma VMware desde el Vcenter Server.
7. Verificación de la configuración.

   Para finalizar la configuración verificamos que la configuración de la cabina es la deseada, y generamos y almacenamos un backups de la correcta configuración actual para su utilización en caso necesario.

4.5. Configuración de la suite VMware vSphere 5

Tras la realización de la configuración de toda la arquitectura física sobre la que se va a sustentar la plataforma virtual, se realiza la implementación y configuración de la plataforma virtual VMware. En este apartado se va a describir el procedimiento de integración de todos los servidores ESXi en el vCenter Server, la configuración de los servicios de red VMware, la configuración del almacenamiento presentado a los ESXi mediante la adición de los datastores disponibles, la verificación del pool de recursos disponible y la adición de las primeras máquinas virtuales resultado de la virtualización de los servidores físicos que ya daban servicio en la empresa. Para el desligue y configuración del entorno virtual se van a seguir los siguientes pasos [3][36][37]:

1. Conexión al vCenter Server
2. Creación del clúster de hosts ESXi
3. Integración de los servidores ESXi en el Vcenter
4. Virtualización de los servidores actuales
5. Supervisión pool de recursos de CPU y memoria RAM de clúster:

A continuación se van a describir con detalle se van a describir con detalle cada uno de los pasos anteriores.

4.5.1. Conexión al vCenter Server

Para la configuración de la suite VMware vSphere 5 es necesaria la conexión al vCenter Server. Para ello, se puede utilizar cualquiera de las interfaces de usuario gráficas que pone a disposición VMware: el VMware vSphere Web Client o el VMware vSphere Client. En nuestro caso, para la administración de la plataforma se va a utilizar el VMware vSphere Client conectando de forma local desde el servidor físico que contiene la instalación del VMware vCenter Server. El acceso a este servidor físico que contiene el vCenter Server siempre se realizará por conexión local (LAN o MPLS) o a través de VPN. Con esto, se proporciona un acceso totalmente seguro a la consola de administración y gestión centralizada de la arquitectura virtual. Para acceder al vCenter Server, se introducen las credenciales de acceso en el VMware vSphere Client y autentica contra la instancia de vCenter Server.

4.5.2. Creación del clúster de hosts ESXi

Una vez autenticado, la primera tarea a realizar es la creación del clúster de hosts ESXi. Para ello, se clica con el botón derecho sobre el *Datacenter* que se creó en el apartado 4.2 y que aparece en la figura 21, y se selecciona la opción *New Cluster*. A continuación, arranca el asistente de configuración del clúster en el que se procede a configurar las siguientes opciones:

- *Cluster Features*. Seleccionamos el nombre del clúster y habilitamos la opción *Turn on vSphere HA* para disponer de la opción de alta disponibilidad en el clúster. También nos da la opción de activar la opción DRS (Distributed Resources Scheduler), que permite distribuir automáticamente el pool de recursos disponibles balanceando y optimizando los recursos en tiempo real. Sin embargo, esta característica no está disponible en la versión de licencia *VMware vSphere Standard 5*, que es la que disponemos, y no la podemos activar (esta característica está disponible en las licencias Enterprise y Enterprise Plus).

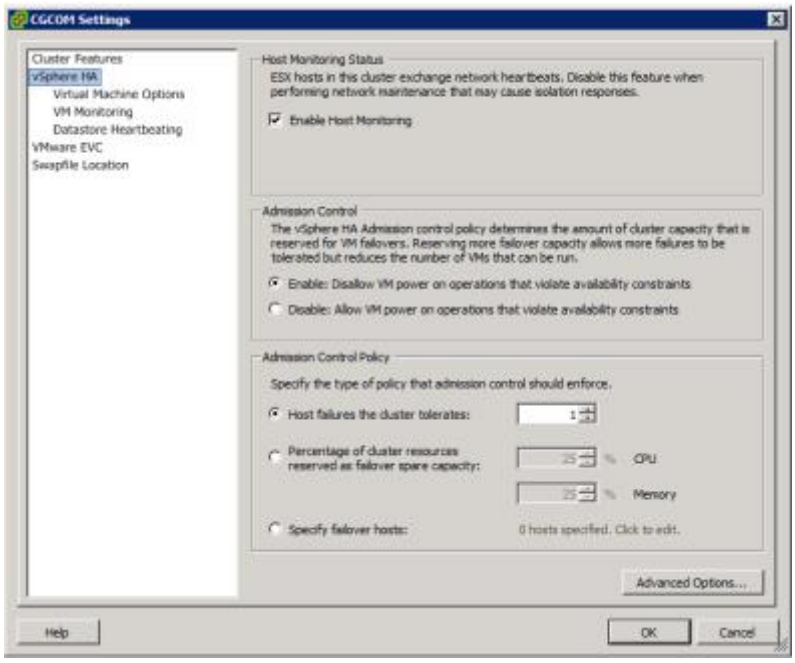


Figura 28: Asistente de creación del clúster

- *vSphere HA*. El siguiente paso en la configuración del clúster son las opciones de alta disponibilidad. *vSphere HA* garantiza la alta disponibilidad de las aplicaciones que se ejecutan en las máquinas virtuales. En caso de fallo del servidor ESXi, las máquinas virtuales afectadas se reinician automáticamente en otros servidores del clúster con suficiente capacidad para ejecutarlas. *vSphere HA* se configura, gestiona y supervisa en vCenter Server, siempre a nivel de clúster, y protege contra fallos de host ESXi, fallos de máquina virtual/sistema operativo

huésped y fallos de aplicación. Para definir los ajustes del servicio vSphere HA se configuran las siguientes opciones:

- *Host Monitoring Status*. Permite realizar un control de la disponibilidad de los hosts ESXi del clúster y debe estar activa para que el servicio *vSphere HA* supervise los fallos y responda ante ellos. Es importante deshabilitar esta opción cuando realizamos tareas de mantenimiento sobre los hosts ESXi para que el sistema no se crea que el host está caído y reinicie las máquinas virtuales en otro host. Cuando la supervisión de hosts está deshabilitada, los hosts se siguen supervisando y, si alguno falla, se informa del evento. La diferencia entre esta situación y cuando la opción esta activada estriba en que en este caso no se realiza ninguna acción.
- *Admission Control*. Se habilita el control de admisión para determinar la cantidad de recursos disponibles que pueden usarse para arrancar máquinas virtuales en un host. La reserva de más capacidad para las caídas de las máquinas permite tolerar más fallos, pero reduce el número de máquinas que pueden ser arrancadas de forma normal en el host ESXi. En nuestro caso, se ha habilitado el control de acceso para no encender máquinas virtuales en operaciones que no cumplan las restricciones de disponibilidad. De este modo, mantenemos la estabilidad global de la plataforma virtual.
- *Admission Control Policy*. La política de control de admisión ayuda a asegurar recursos suficientes para lograr el óptimo funcionamiento de alta disponibilidad en el clúster. En nuestro caso, se ha fijado que el clúster tolere la caída de un host, como ya se tuvo en cuenta durante el diseño de los recursos de la arquitectura virtual. De este modo, como ya se calculó, la arquitectura virtual debe tolerar sin problemas la caída de un host del clúster y el servicio vSphere HA se encargará de ubicar las máquinas virtuales alojadas en el host caído, mediante vMotion, con pérdida mínima de servicio. De todos modos, según se vayan desplegando las máquinas virtuales se puede ir ajustando este valor si fuera necesario.
- *Virtual Machine Options*. En esta pestaña se fijan las opciones de reinicio que queremos fijar para las máquinas virtuales en el clúster cuando se produce un fallo en el host que las alberga. La prioridad de reinicio, es decir, el orden relativo en que arrancarán las máquinas virtuales tras un fallo de host, se ha establecido en *medium* como indica la política por defecto, lo que quiere decir que a nivel de clúster se van a arrancar todas las máquinas con la misma prioridad. A medida que se vayan creando las máquinas virtuales de los diferentes proyectos a implantar, se puede ir ajustando

este valor si fuera necesario.

La opción de configuración *Host isolation response* determina qué pasa con las máquinas virtuales cuando un host pierde la red de gestión, pero sigue funcionando (estado *isolate*). En nuestro caso mantenemos la opción por defecto, *Leave Powered on*, y mantenemos las máquinas virtuales encendidas.

- *VM Monitoring*. Esta opción permite la monitorización de las máquinas virtuales dentro del clúster. Estas características permiten reiniciar de forma automática las máquinas virtuales si se pierde la conexión con ellas a través del sistema de control (*heartbeats*) que desarrolla VMware. En nuestro caso, se mantendrá desactivada esta opción porque se prefiere realizar el control del reinicio y el estado de las máquinas virtuales mediante un sistema de monitorización especifico y desarrollado para ello que controla tanto los recursos del servidor virtual, su estado y el estado de funcionamiento de las aplicaciones que alberga, y no solo se basa en posibles pérdidas de respuesta que pueden provocar falsos positivos.
- *Datastore Hearthbeating*. vSphere HA usa *datastores* para monitorizar hosts y máquinas virtuales cuando se producen fallos en la red de gestión. vCenter Server selecciona 2 datastores por cada host usando la política y preferencias indicadas en esta pestaña de configuración. En nuestro caso, se ha seleccionado para que sea automáticamente vSphere HA quien elija los *datastores* libremente para realizar la monitorización.

- *VMware Enhanced vMotion Compatibility* (EVC). EVC es una funcionalidad de clúster proporcionada por VMware que impide el fallo de migraciones de vMotion a causa de incompatibilidades de CPU entre los hosts ESXi que componen el clúster. EVC se asegura de que todos los hosts de un clúster presenten las mismas características de CPU a las máquinas virtuales, aunque las CPU de los hosts sean en realidad diferentes. Una vez habilitada, EVC asegura que únicamente los hosts compatibles con los que componen el clúster podrán ser añadidos al mismo. Todos los hosts de un clúster EVC deben cumplir los siguientes requisitos:
  - Usar CPU de un único proveedor (ya sea Intel o AMD).
  - Estar conectados a Vcenter Server.
  - Estar habilitados para la virtualización de hardware (Intel VT o AMD-V).
  - Estar configurados para la migración vMotion.

  Esta característica es fundamental y de vital importancia en la arquitectura virtual que se está

configurando para el funcionamiento óptimo del VMware vMotion, ya que los servidores físicos que componen el clúster pertenecen a 2 fabricantes distintos, IBM y DELL, y aunque tienen características de CPU similares sin esta característica habilitada no podría ejecutarse el vMotion entre máquinas virtuales que funcionan en los hosts ESXi de diferente fabricante. Por ello, se habilita EVC para host con procesadores Intel® que son los se utilizarán en los servidores físicos ESXi. Dentro del *VMware EVC Mode* se selecciona la opción Intel® Xeon Core 2 correspondiente a las características de nuestros servidores como se muestra en la siguiente figura:

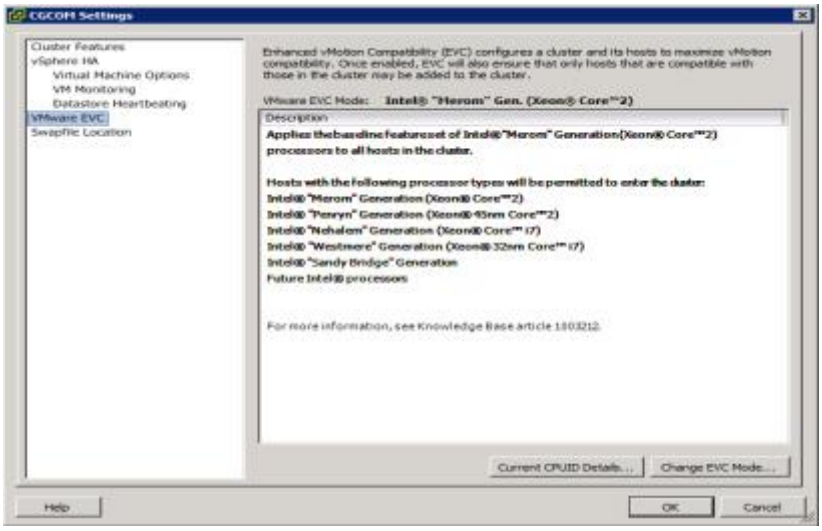


Figura 29: EVC con Intel® Xeon Core 2

- *Swapfile Location*. Esta opción permite fijar la política para los ficheros de swap de las máquinas virtuales de clúster. Podemos ubicar el archivo de paginación de las máquinas virtuales en la propia carpeta de la máquina virtual o en una LUN destinada a esta funcionalidad. En nuestro caso, seleccionamos la opción de almacenar dichos ficheros en el mismo directorio que el resto de ficheros de la máquina virtual.

Tras esto finalizamos el asistente y ya tenemos creado el clúster de la arquitectura virtual y, en este punto, ya podemos añadir los diferentes ESXi que formarán parte de dicho clúster.

4.5.3. Integración de los servidores ESXi en el vCenter Server

En este apartado se va a describir el procedimiento seguido para añadir al clúster los hosts ESXi. En este punto cabe resaltar que, aunque la configuración detallada en el capítulo 4 la hemos referido

siempre a 6 host ESXi, en este punto de la instalación y configuración solo se dispone de los 4 servidores físicos adquiridos exclusivamente para la plataforma virtual y faltaría por virtualizar los 2 servidores DELL con los que ya se contaba en la situación inicial y que estaban ofreciendo servicios de producción en este momento. La razón de realizarlo de este modo, como se describirá más adelante, es debida a que podemos migrar a la plataforma virtual clones de los servidores físicos en producción reduciendo el tiempo de interrupción del servicio y manteniendo intacta la configuración y los servicios existentes en dichos servidores. Por ello, en primer lugar, crearemos un clúster de 4 ESXi y posteriormente, una vez migrados los servidores físicos a la plataforma virtual como máquinas virtuales que corren en alguno/s de estos ESXi ya configurados, se procederá a incorporar estos servidores en el clúster. Las tareas de paso de físico a virtual de los servidores en producción serán descritas en un apartado específico posterior dentro de este apartado.

Para la integración de los ESXi seguimos el siguiente procedimiento [3]:

1. Se clica con el botón derecho sobre el clúster creado en el apartado anterior y se selecciona la opción *Add host*. A continuación, aparece un asistente que nos guiará en el proceso para añadir un nuevo host al clúster.
2. Para conectar el host al clúster se proporciona el nombre o la IP del mismo y la contraseña de administrador fijada durante la instalación del VMware vSphere 5.0 Update 1 que se realizó en el apartado 4.2. La adición del host al clúster se realiza a través de servicios VMware que buscan al candidato dentro de la red interna con las credenciales e IP proporcionados. Además, durante este proceso vCenter Server instala un agente en los hosts ESXi a través del cual se comunica y administra los hosts.
3. El host es añadido al cluster y es mostrado un resumen con información de las máquinas virtuales que se ejecutan actualmente en ese host (en este caso ninguna).
4. En la siguiente pantalla del asistente permite cargar las licencias a los hosts según se vayan añadiendo. Para ello, cargamos en primer lugar todas las licencias adquiridas en VMware para nuestra plataforma virtual:
   - 1 Standard Acceleration kit para 8 procesadores (con 32 GB VRAM por cada procesador).
   - 4 licencias VMware vSphere 5 Standard para 1 procesador (con 32 GB VRAM por cada procesador).

   Una vez añadidas se van asignando las licencias para 2 CPU por cada host añadido. VMware te permite añadir el host con una licencia en modo evaluación, que dura 60 días, y luego fijar la licencia definitiva antes de su expiración.

5. En la última ventana, el asistente da la posibilidad de elegir la opción *Lockdown Mode*, el modo bloqueo, que inhabilita el acceso remoto de la cuenta root. Una vez el vCenter Server toma el control del host, como de forma predeterminada no existen cuentas de usuario local en el sistema ESXi y estas cuentas solo se pueden crear antes de habilitar el modo de bloqueo, el acceso remoto queda inhabilitado. Este modo garantiza que el host sea siempre y únicamente gestionado a través del vCenter Server. En nuestro caso habilitaremos esta opción para garantizar la seguridad al impedir el acceso remoto a los hosts ESXi. Cabe resaltar que esta opción puede ser deshabilitada de forma temporal para realizar tareas de mantenimiento en los hosts ESXi accediendo de forma remota desde otras herramientas que no proporciona el vCenter Server y que analizaremos en los próximos capítulos.
6. Se finaliza el asistente y el host queda añadido al clúster VMware de la plataforma virtual pasados unos segundos.

El proceso anterior es repetido para los otros 3 ESXi disponibles. En la imagen siguiente se muestra el clúster de la arquitectura virtual tras completar la integración de los 4 ESXi en el clúster:

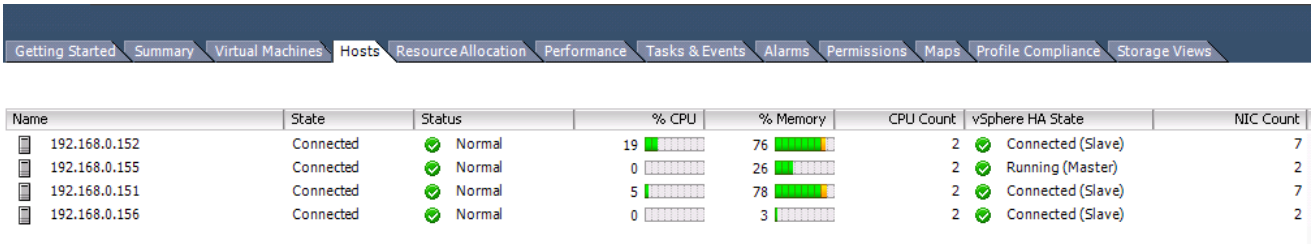


Figura 30: Clúster con los 4 host ESXi integrados

Cabe resaltar en la imagen anterior el estado del servicio vSphere HA configurado en el clúster donde puede visualizarse el host dentro del clúster que actúa como maestro.

A continuación, se van a describir las tareas llevadas a cabo para la realización de la configuración básica de cada ESXi. Para ello, se va a configurar en cada ESXi una serie de características importantes que están disponibles en la pestaña *Configuration* de cada ESXi. Dentro de esta pestaña existe una división para la configuración entre características hardware y características software (puede visualizarse en la figura 31 que se muestra en la página siguiente). Posteriormente, se va a realizar un recorrido descriptivo por el resto de pestañas informativas que vCenter Server ofrece de cada ESXi.

HARDWARE

Processors: Muestra información sobre las características de los procesadores físicos del ESXi seleccionado. No permite configuración, sino que ofrece datos informativos.

Memory: Muestra información sobre la cantidad de memoria física instalada en el ESXi. No permite configuración, sino que ofrece datos informativos.

Networking: Permite la configuración de los servicios de red en los servidores ESXi. El procedimiento para la realización de la configuración de los servicios de red en cada ESXi es expuesto a continuación:

1. Configuración predeterminada del switch virtual estándar *vSwitch0*.

La arquitectura de red de un host ESXi gira en torno a la creación y configuración de los switches virtuales (vSwitch). Para realizar la configuración de un switch virtual estándar, se utiliza la opción *Networking* de la pestaña *Configuration* de cualquier host. Como puede verse en la figura 31, al crear el vSwitch estándar, se crean por defecto 2 grupos de puertos, uno de cada tipo: un grupo de puertos para máquinas virtuales que se denomina *VM Network* y un grupo de puertos del VMkernel que se denomina *Management Network*, bajo la interfaz VMkernel vmk0 y la VLAN ID 10 como se realizó durante la instalación del ESXi:

Figura 31: Configuración predeterminada de un switch virtual estándar.

Una buena práctica es mantener las redes de máquinas virtuales y las redes de gestión independientes por motivos de rendimiento y seguridad. Para aislar la red de gestión del resto de redes, se ha utilizado la VLAN con ID 10 como ya se definió durante el diseño de la red de la arquitectura virtual.

Para la configuración del switch virtual estándar utilizaremos la opción *Properties* y se abrirá un asistente de configuración para la adición de grupos de puertos y configuración de adaptadores de red físicos.

2. Creación del *NIC Teaming*. Mediante el teaming se agrupa la capacidad de las 2 interfaces de red como si fuera un único canal. Sobre este canal se tendrán las interfaces virtuales de gestión

y vMotion. Con esto se consigue **alta disponibilidad:** si se estropea un puerto ethernet se dispondrá todavía de un canal de 1 GB sobre el que seguirán funcionando las 2 interfaces virtuales; **mayor capacidad**: ya que cuando no se utilice la red gestión se utilizará todo para mandar datos; y **balanceo de carga**: se produce balanceo de carga entre las interfaces que componen el *Teaming* a nivel de número de conexiones, no a nivel de cantidad de tráfico. Para ello se accede en la Pestaña *Network Adapters* y se añade el otro adaptador disponible de los 2 que se encuentran físicamente conectados en cada host ESXi como se estableció en el diseño y se conectó durante la instalación. En la figura 33 anterior ya aparece realizado el *NIC Teaming* como puede visualizarse en la zona denominada *Physical Adapters*.

3. Definición de las carácterísticas del switch.
    a. Grupo de puertos: En esta pestaña se añadirán todos los grupos de puertos, tanto para tráfico entre las máquinas virtuales como para los grupos de puertos del VMKernel. Además, en esta pestaña definimos las características del vSwitch mediante la opción *Edit*:

    <u>*General*</u>: Se mantiene el número de puertos disponibles por defecto del *vSwitch0* en 120, ya que este número puede ser aumentado según se necesite hasta un valor máximo de 4088. Estos puertos serán utilizados para conexiones de máquinas virtuales y para tarjetas de interfaz de red físicas, denominadas uplinks. Por defecto, siempre se reservan 8 puertos para grupos de puertos del VMkernel, número que se suma al indicado anteriormente.

    <u>*Políticas de Red*</u>*:* Pueden definirse 3 políticas de red a nivel de switch virtual (en este punto de la configuración) o luego más específicamente a nivel de grupo de puertos. En nuestro caso, se han definido todas las políticas de red a nivel del switch virtual. Las 3 políticas que se pueden definir son:

    - Seguridad: Permiten configurar opciones de seguridad de nivel 2 de Ethernet en el switch virtual estándar y en los grupos de puertos. En nuestro caso, se configuran las opciones por defecto: Modo Promiscuo (Rechazar), cambios de dirección MAC (Aceptar) y Transmisiones manipuladas (Aceptar). En general estas políticas ofrecen la opción de prohibir ciertos comportamietno que podrían poner en peligro la seguridad y que podrían ajustarse en cualquier momento.
    - Traffic Shapping: Esta política permite controlar el ancho de banda de red de una máquina virtual. Esta opción no ha sido configurada en la arquitectura

virtual por no ser necesaria hasta este momento, por lo que permanecerá deshabilitada. Se utiliza sobre todo en aplicaciones donde el control de ancho de banda es crítico para el correcto funcionamiento de las mismas.

- NIC teaming: Estas políticas permiten determinar como distribuir el tráfico de la red entre los adaptadores y como redireccionarlo en caso de fallo de un adaptador. Además incluyen detección de fallo de red, notificación de switches y conmutación por error. Estas políticas aplican únicamente al tráfico de salida.

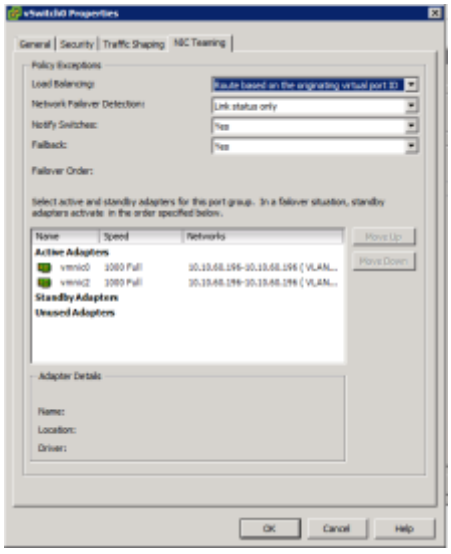


Figura 32: Configuración del NIC Teaming.

Como se muestra en la figura anterior, la política de balanceo de carga para el tráfico saliente que se ha seleccionado ha sido *Routed based on the originating virtual port ID*. Este método distribuye de forma estática los puertos disponibles de las máquinas virtuales asignándolos a los enlaces ascendentes (uplinks). Esta asociación se mantiene mientras no se produzca un error. Es la opción de balanceo por defecto y es un método simple y rápido que no exige que VMkernel examine la trama para obtener la información necesaria.

La detección y gestión de los fallos de red la realiza el VMKernel que supervisa el estado del enlace únicamente o el estado del enlace y la señalización. Se puede notificar a los switches si se produce un evento de conmutación por error o si se conecta una nueva tarjeta de red virtual. La conmutación por error se implementa por VMkernel según parámetros configurables:

- Conmutación por recuperación: indica la forma en que el adaptador físico vuelve a la actividad tras recuperarse de un fallo.

- Opción de balanceo de carga: Se puede utilizar un orden explítico de conmutación por recuperación.

En nuestro caso, como puede verse en la figura 32, las opciones configuradas son: detección de fallo de red de enlace únicamente, notificación de switches y conmutación por recuperación (el adaptador que ha fallado vuelve al servicio activo de inmediato, desplazando al adaptador en espera que ocupó su lugar en el momento del fallo).

b. Propiedades de los adaptadores de red.

En la pestaña *Properties* del switch virtual revisamos la velocidad y la características dúplex de los 2 adaptadores físicos conectados a cada host ESXi para que sean los correctos y para que todos dispongan de los mismos parámetros en todos los hosts ESXi. Los parámetros que se utilizan como mejores prácticas en los adaptadores Ethernet son *Configured Speed*, *Duplex* y *Auto negotiate* porque es parte del estándar Gigabit.

4. Definición de las redes de datos para el tráfico de las máquinas virtuales.

A continuación, se van a añadir al switch virtual vSwitch0 los grupos de puertos de máquina virtual que van a permitir el tráfico de las máquinas virtuales que se necesitan en cada host teniendo en cuenta las VLANs ID definidos en el apartado 3.3.2 de diseño ethernet. Teniendo en cuenta esto, se clica en *Properties* y a continuación en *Add Network Wizard* y se selecciona el tipo de conexión a añadir, de gestión o de datos:

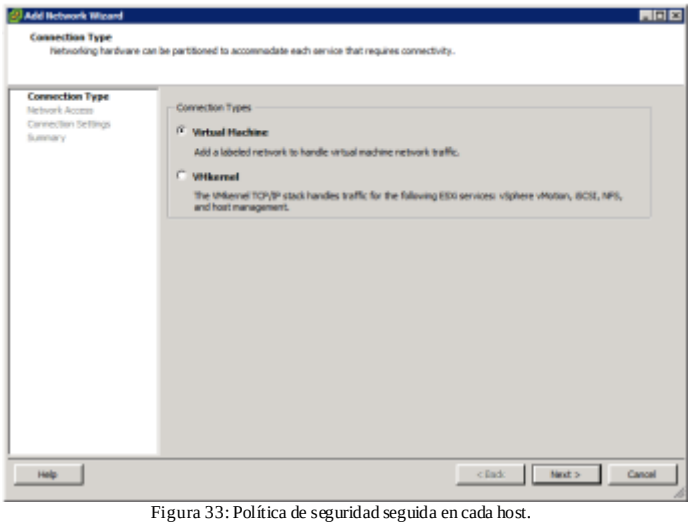


Figura 33: Política de seguridad seguida en cada host.

En las conexiones de datos se van añadiendo los distintos grupos de puertos constituyendo las distintas subredes e identificándolas con el VLAN ID definido en la tabla 3:

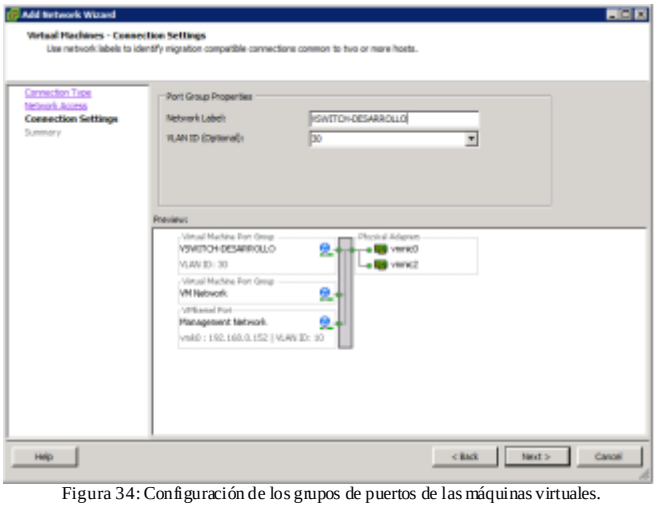


Figura 34: Configuración de los grupos de puertos de las máquinas virtuales.

De este modo, se van añadiendo todas las VLAN de datos identificándolas con su nombre y su VLAN ID: VSWITCH-DESARROLLO, VSWITCH-PREPRODUCCION, VSWITCH-PRODUCCION, VSWITCH-WEBS, VSWITCH-SERVICIOS_TEST, VSWITCH-SERVICIOS_PRODUCCION, VSWITCH-ADMINISTRACION_TEST, VSWITCH-ADMINISTRACION_PRODUCCIÓN, VSWITCH-BBDD_TEST y VSWITCH_BBDD_PRODUCCION. Es importante que las conexiones creadas en los switches bajo el mismo VLAN ID tenga el mismo nombre para que pueda realizarse la migración de las máquinas sin problemas reconociendo la misma red durante el VMware vMotion.

5. Realizamos la configuración de la red de gestión.

A continuación, se van a añadir al switch virtual vSwitch0 las distintas redes de gestión, a través de las cuales se gestiona el tráfico de administración y control del VMkernel. En cada vSwitch estándar correspondiente a cada host ESXi de la arquitectura virtual vamos a disponer de 2 grupos de puertos del VMkernel:

a) Red de gestión de tráfico

Para ello, se edita el grupo de puertos "Management Network" que se crea por defecto con la creación del vSwitch en cada ESXi. Se modifica el nombre de la red a "Red de Gestión" y se activa la opción *Management Traffic* para controlar el tráfico a través de esta red de gestión. Para añadir esta característica clicamos sobre la opción vMotion de la pestaña de *Propiedades* de esta conexión.

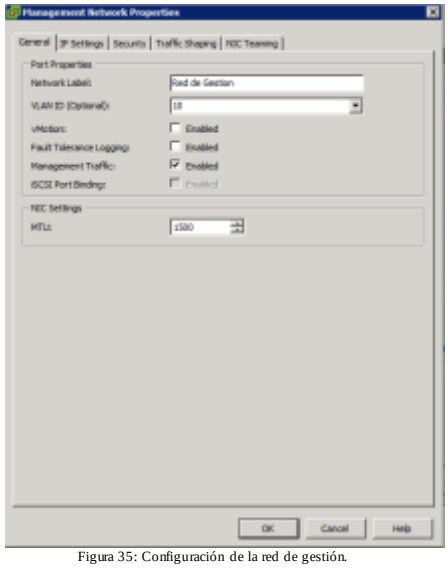


Figura 35: Configuración de la red de gestión.

Como puede observarse en las figuras 31 y 34, los grupos de puertos de VMkernel comprenden un puerto en el vSwitch y una interfaz de red VMkernel, denominada *vmknic*. Además, la interfaz requiere una dirección IP que es usada para gestión o acceso del VMkernel. En el caso de la Red de Gestión de cada ESXi, la vmknic es la vmk0 y la IP de la interfaz coincide con la asignada a cada ESXi en la tabla 7, IP que pertenece a la VLAN con VLAN ID 10. La información de dicha IP puede visualizarse o modificarse en la pestaña *IP Settings*. Las tres pestañas restantes de la ventana de configuración no se modificarán porque tomarán las configuraciones realizadas a nivel de vSwitch.

b) Red de vMotion

La red de vMotion la vamos a implementar sobre la misma Red de Gestión ya definida en el punto anterior. Para añadirle la característica de vMotion, simplemente editamos el grupo de puertos de gestión ya definidos y activamos la casilla que considera esta red para la realización de las tareas de vMotion.

Storage: Permite la configuración del almacenamiento en los servidores ESXi. A través de esta opción se permite añadir al host los *datastores* VMFS presentados desde la cabina de almacenamiento. Cada host ESXi tendrá acceso a las LUN que le hayan compartido o presentado desde la cabina de almacenamiento como se detalló en el apartado 4.4.2. Para añadir los datastores se utiliza la opción *Add Storage*. Al clicar sobre esta opción se inicia el asistente para añadir los *datastores* VMFS para el almacenamiento. Dentro del asistente, el procedimiento para añadirlos es el siguiente:

1. Seleccionamos como tipo de almacenamiento disco/LUN.

2. Seleccionamos una LUN disponible.
3. Especificamos el nombre del datastore.
4. Especificamos el tamaño máximo del datastore: si queremos añadir la LUN completa o solo parte.

Repetimos el procedimiento para cada LUN presentada desde la cabina hasta hacer disponibles todas a las que tiene acceso cada ESXi. La opción *Rescan All* te permite resincronizar volúmenes o datastores VMFS con los que se haya perdido conexión de forma temporal. En la opción *Storage* también se muestra información detallada de cada datastores VMFS al que se tiene acceso. En la siguiente figura se muestra información de los datastores VMFS disponibles:

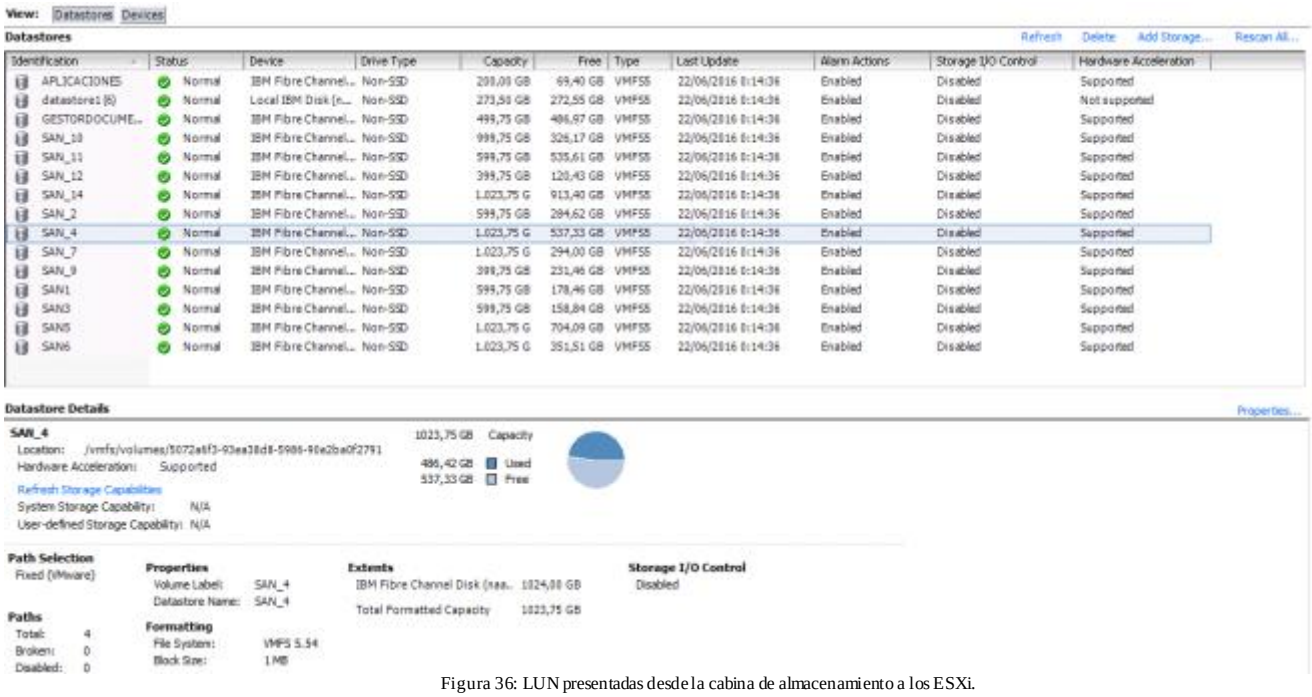


Figura 36: LUN presentadas desde la cabina de almacenamiento a los ESXi.

En la figura anterior puede verse el nombre identificativo de cada *datastore*, que son del tipo VMFS versión 5, que los dispositivos que permiten la conexión con estos *datastore* son Fiber Channel, la capacidad, el espacio libre, el último acceso, etc. Cabe resaltar que el Storage I/O Control esta deshabilitado en todos los datastores ya que no está disponible en la licencia VMware vSphere Standard 5. Está disponible en las licencias Enterprise y Enterprise Plus.

En la parte de abajo de la imagen se muestran las características de una de las LUN, en este caso la denomina SAN_4. Entre ellas destacan su acceso redundado *multipathing* (4 *caminos*), la selección del camino que se realiza (política Fixed), el sistema de fichero (VMFS 5.54) y el tamaño de bloque (1 MB). vSphere 5 ofrece mecanismos de selección de ruta nativa, balanceo de carga y conmutación por error. Las políticas de selección de ruta que ofrece VMware para Fiber Channel son:

- Escalabilidad: Round Robin, que es una política de múltiples rutas que balancea la carga entre rutas. El host usa un algoritmo de selección de ruta que alterna por todas las rutas disponibles.
- Disponibilidad:
    - Most Recently Use (MRU): el host utiliza la última ruta al disco hasta que deja de estar disponible, es decir, el host no cambia a otra ruta hasta que esta deja de estar disponible. Se realiza una conmutación por error en una nueva ruta. MRU es la política predeterminada y obligatoria para los dispositivos de almacenamiento activo-pasivo.
    - Fixed: el host siempre utiliza la ruta preferida al disco en caso de que esté disponible. Si el host no puede acceder al disco mediante la ruta preferida prueba las rutas alternativas. Esta política es la predeterminada para los dispositivos activo-activo.

Como se ha comentado anteriormente y al disponer de una cabina activo-activo, se ha seleccionado la política Fixed para el balanceo de carga que es una política activo-activo pero más conservadora que la Round Robin, anteponiendo disponibilidad en lugar de escalabilidad. En el futuro, para algún datastore concreto se puede cambiar la política a Round Robin si se necesita mayor rendimiento. Para configurar estas opciones hay que seleccionar el *datastore* determinado y clicar sobre *Properties* y a continuación clicar sobre *Manage Paths*.

Storage adapter: Esta opción no permite realizar ninguna configuración, pero muestra información sobre los adaptadores de almacenamiento conectados al host ESXi y de los recursos de almacenamiento conectados a esos adaptadores. El VMKernel detecta todos los dispositivos PCI cuando arranca el host ESXi. De forma predeterminada VMkernel busca los LUN de 0 a 255 de cada destino (un total de 256 LUN). ESXi no puede detectar los LUN que tengan un número ID de LUN superior a 255. En la siguiente figura se muestran los dispositivos de almacenamiento y las LUN detectadas de la cabina de almacenamiento IBM DS3524:

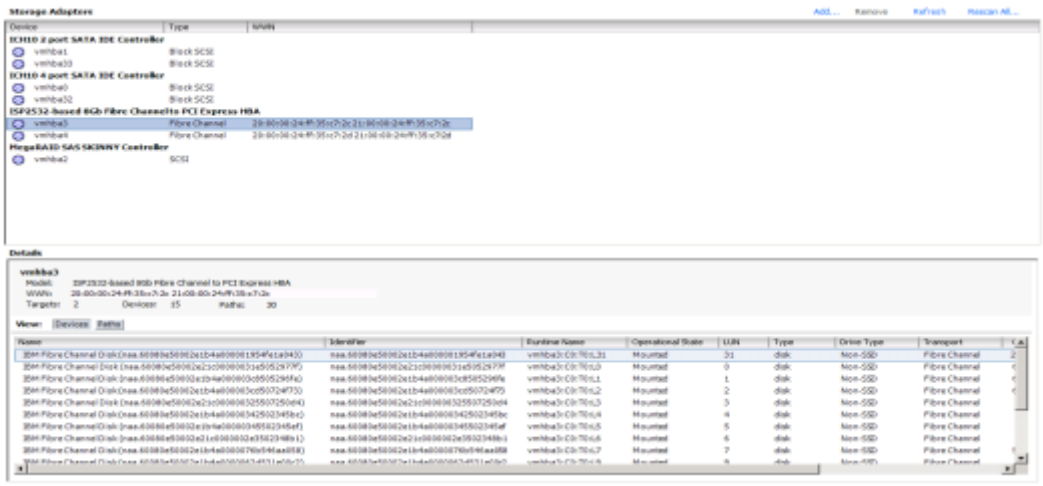


Figura 37: Adaptadores fiber channel del host y dispositivos fiber channel detectados.

Network adapter: Esta opción no permite realizar ninguna configuración, pero muestra información sobre los adaptadores de red Ethernet conectados al host ESXi y de si están activos o no.

Advanced Settings: VMware ESXi proporciona opciones de configuración avanzada que afectan al funcionamiento de varios componentes y que permiten alterar el funcionamiento normal de estos. Las opciones de configuración avanzada pueden ser revisadas y modificadas en un host ESXi utilizando vSphere Client, PowerCLI, la interfaz de la línea de comandos o la consola local. VMware recomienda que estas opciones sean alteradas de su comportamiento por defecto bajo la supervisión del equipo de soporte de VMware. En nuestro caso no realizamos ninguna configuración de este tipo.
Power Management: Permite definir políticas de apagado y encendido de máquinas virtuales para el ahorro de energía eléctrica durante determinados períodos.

SOFTWARE

Licensed Features: En esta pestaña podemos ver las características y el tipo de la licencia disponible en el ESXi, así como los productos disponibles asociados a la licencia. En la siguiente imagen podemos ver las características de la licencia VMware vSphere 5 Standard disponible:

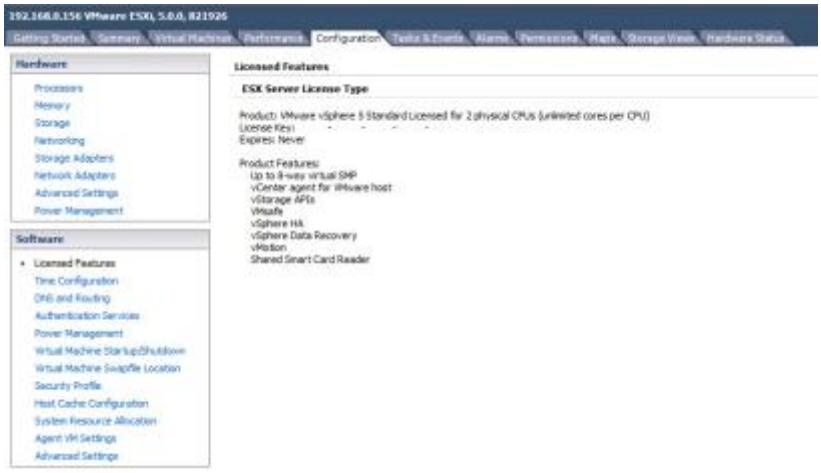


Figura 38: Característica de la licencia disponible en cada host ESXi.

Time configuration: En esta pestaña se realiza la configuración del host como cliente de protocolo de tiempo de red NTP. Configuramos cada uno de los hosts para que se sincronice en fecha y hora con algún servidor NTP público conocido y fiable (ntp.ubuntu.com). Para ello es necesario habilitar el cliente NTP en cada servidor ya que viene deshabilitado por defecto e indicamos que se arranque de forma automática al arrancar el ESXi. Esto es importante entre otras cosas:

- Para realizar gráficas de rendimiento precisas.

- Para que en los mensajes de los registros se indique fecha y hora con precisión.
- Para que las máquinas virtuales puedan sincronizarse con el ESXi para disponer de una fecha y hora actualizadas. Esto es importante para nuestra empresa sobre todo en bases de datos que deben registrar eventos.

DNS and Routing: Esta pestaña permite configurar o modificar los servidores DNS primario y secundario. Como en mi empresa no disponemos de servidor DNS propio fijamos unos servidores DNS externos estables como los de nuestro proveedor de registro de dominios. El DNS es importante para los servicios del ESXi que van a utilizar nombres, como por ejemplo el servicio NTP configurado anteriormente.

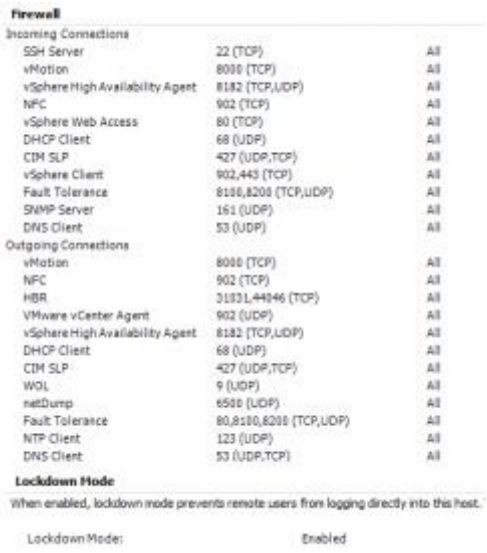
Authentication Services: En este apartado permite configurar la autenticación de los usuarios en los hosts ESXi. Siguiendo las recomendaciones de *mejores prácticas de VMware* [9], se utilizará casi exclusivamente vSphere Client y Vcenter Server para gestionar los host ESXi. Para resolver determinados problemas y situaciones concretas o aplicar configuraciones específicas se utiliza otro tipo de conexión, como por ejemplo SSH. Durante estas situaciones, se habilitará el servicio únicamente el tiempo que dure la actuación y siempre conectándose por interfaz local desde el servidor que contiene la instalación del vCenter Server.

Power Management: Esta opción permite establecer varias políticas de gestión de encendido en el ESXi seleccionado. Se utiliza sobre todo cuando se quiere balancear o ahorrar el consumo energético.

Virtual Machine Startup/Shutdown: Esta pestaña permite configurar el encendido o el apagado automático de las máquinas virtuales sincronizado con el encendido y el apagado del host ESXi. No configuramos esta opción.

Virtual Machine Swapfile Location: Este apartado permite configurar la localización de los ficheros de swap de las máquinas virtuales que están funcionando dentro del host seleccionado. Esta configuración ya fue fijada en la configuración del clúster y la configuración del clúster prevalece sobre la configuración de los hosts que forman parte del mismo.

Security Profile: Esta pestaña permite configurar el perfil de seguridad de cada host ESXi. En este apartado se configura el firewall de seguridad que lleva integrado cada ESXi. La configuración recomendada es evitar que los clientes remotos accedan a los servicios del host e impedir que los clientes locales accedan a los servicios de host remotos. Esta es la política de configuración seguida por nuestra empresa y ha sido habilitada al seleccionar la opción la opción *Lockdown Mode* al incluir el host en el clúster. Para garantizar la integridad del host casi la totalidad de los servicios viene deshabilitada por defecto y solo están habilitados aquellos necesarios para el propio funcionamiento de los servicios VMware vSphere.



Firewall

Incoming Connections		
SSH Server	22 (TCP)	All
vMotion	8000 (TCP)	All
vSphere High Availability Agent	8182 (TCP,UDP)	All
NFC	902 (TCP)	All
vSphere Web Access	80 (TCP)	All
DHCP Client	68 (UDP)	All
CIM SLP	427 (UDP,TCP)	All
vSphere Client	902,443 (TCP)	All
Fault Tolerance	8100,8200 (TCP,UDP)	All
SNMP Server	161 (UDP)	All
DNS Client	53 (UDP)	All
Outgoing Connections		
vMotion	8000 (TCP)	All
NFC	902 (TCP)	All
HBR	31031,44046 (TCP)	All
VMware vCenter Agent	902 (UDP)	All
vSphere High Availability Agent	8182 (TCP,UDP)	All
DHCP Client	68 (UDP)	All
CIM SLP	427 (UDP,TCP)	All
WOL	9 (UDP)	All
netDump	6500 (UDP)	All
Fault Tolerance	80,8100,8200 (TCP,UDP)	All
NTP Client	123 (UDP)	All
DNS Client	53 (UDP,TCP)	All

Lockdown Mode

When enabled, lockdown mode prevents remote users from logging directly into this host.

Lockdown Mode: Enabled

Figura 39: Política de seguridad seguida en cada host.

Host cache configuration: Esta pestaña permite visualizar o fijar la cantidad de espacio en volúmenes SSD disponibles que pueden ser usados para espacio swap. La arquitectura virtual que se está configurando no cuenta con discos SSD por lo que esta opción no fue configurada.

System Resource Allocation: Este apartado permite realizar un ajuste de la localización de los recursos para el host ESXi seleccionado. En este punto de la configuración no hay que realizar ninguna configuración en este apartado.

Agent VM Settings: Este apartado permite añadir máquinas virtuales ya configuradas, que proporcionan servicios adicionales de VMware, las proporciona el propio fabricante y añaden a la infraestructura funcionalidad muy específica. En la arquitectura virtual a configurar no se dispone de ninguna máquina virtual de este tipo.

Advanced Settings: Esta pestaña proporcionada un acceso directo para fijar todas las configuraciones del host seleccionado. Proporciona una visión general y rápida de la configuración que dispone el host seleccionado.

Como se desprende de la descripción anterior, VMware proporciona todas las herramientas que la mayoría de los administradores necesitan para gestionar los hosts ESXi.

4.5.4. Virtualización de los servidores físicos actuales

En este apartado se va a describir el procedimiento de migración de los servidores físicos con los que ya se contaba en la empresa para incorporarlos como servidores hosts ESXi dentro de la arquitectura virtual. Cabe resaltar que la migración de los servidores físicos a la arquitectura virtual,

tarea que se conoce comúnmente como conversión de físico a virtual (physical-to-virtual (P2V)), lleva implícito en nuestro caso una interrupción de la prestación del servicio. Por ello, desarrollamos esta tarea a horas donde no se registra actividad en los servicios prestados desde estos servidores. El procedimiento consta, a grandes rasgos, de dos fases secuenciales:

Primera fase [38]: En esta primera fase se realiza una migración de los servidores físicos para convertirlos en máquinas virtuales que corren dentro de la arquitectura virtual. Para la realización de esta operación se va utiliza la herramienta gratuita que proporciona VMware para la realización de estas operaciones y que es denominada VMware vCenter Converter Standalone Client 5. Los beneficios principales que aporta esta herramienta son expuestos a continuación:

- Convierte máquinas físicas que estén ejecutando Windows o Linux de una manera sencilla y sin tiempo de parada.
- Convierte imágenes de terceros de máquinas como pueden ser Parallels Desktop, Symantec Backup Exec System Recovery, Norton Ghost, Acronis, StorageCraft, Microsoft Virtual Server o Virtual PC, y Microsoft Hyper-V Server a máquinas virtuales VMware.
- Permite una gestión centralizada de conversiones de máquinas virtuales o físicas, así podremos gestionar desde una única consola la migración de varias máquinas al mismo tiempo.
- Agrega una fiabilidad máxima al realizar la copia mediante un snapshot del sistema operativo de la máquina de origen, antes de empezar a migrar.
- Permite clonaciones sin parada de servicio, sin tener que reiniciar el servidor origen.

A continuación, se va a presentar el escenario de trabajo a considerar para el desarrollo correcto de la migración.

- En la migración P2V es necesario un equipo puente en el cual se realiza la instalación del VMware Vcenter Converter y que debe encontrarse en la misma subred que los equipos a migrar. Este equipo hará de puente entre el servidor físico que queremos virtualizar (origen) y el servidor de virtualización ESXi (destino) donde crearemos la máquina virtual. Este equipo será un servidor de conversión.
- Los servidores físicos a migrar deben tener conectividad con el clúster de servidores ESXi para permitir su migración directa a la arquitectura virtual, en la que se alojará una máquina virtual que será un clon del servidor físico original.

Teniendo en cuenta los condicionantes anteriores, utilizaremos el servidor físico donde se encuentra instalado el VMware vCenter Server para realizar la instalación del VMware vCenter Converter

Standalone Client 5 y cambiaremos el direccionamiento IP de los servidores físicos a migrar asignándoles una IP de la subred 192.168.0.0/24 desde la que existe conectividad directa a nivel LAN con los ESXi y el VMware vCenter Server.

Tras la definición del escenario de trabajo, se procede a la realización del procedimiento para la migración P2V de los servidores:

1. Instalación del VMware vCenter Converter Standalone Client 5 descargando dicha herramienta disponible en la cuenta de la empresa en VMware.
2. Tras su descarga se procede a la instalación de la herramienta. La instalación dispone de un asistente que ejerce guía y hace que la misma sea muy sencilla y quede realizada en pocos segundos.
3. Arranque del programa vCenter Converter y se selecciona la opción *Converter Machine*. A continuación, se completa la información necesaria tanto en el servidor físico origen como del servidor virtual destino:

    - Servidor físico origen: *Powered-on machine* (convierte una máquina física encendida en máquina virtual), la IP o nombre de los servidores físicos, las credenciales de acceso de un usuario administrador y el tipo de sistema operativo.
    - Servidor virtual destino: *VMware Infraestructure virtual machine* (el destino es una máquina virtual dentro de una infraestructura virtual), IP del servidor ESXi que va a alojar al servidor físico virtualizado y las credenciales de acceso al servidor ESXi.

4. Tras establecer la conexión entre origen y destino, el asistente del VMware vCenter Server permitirá asignar los recursos de memoria RAM, CPU y disco para que la migración P2V se complete con éxito.
5. Tras el procedimiento anterior el asistente se completa y comienza el proceso real de migración que, tras algunas horas, dependiendo del tamaño del disco, se completa con éxito.
6. Utilizando el VMware vSphere Client se procede a conectarse con el vCenter Server y se detectan los dos nuevos servidores virtuales que se encuentran alojados bajo el ESXi destino de la migración. Finalmente, ambos servidores son arrancados para que los servicios comiencen a proporcionarse de nuevo.

Tras completar el proceso anterior, los servidores físicos estaban disponibles en la plataforma virtual en forma de máquina virtual. Se ajustó la presentación de los servicios al exterior a través de NAT en

el Firewall y finalmente los servicios interrumpidos fueron levantados con éxito en la plataforma de virtualización.

Segunda fase: Las tareas desarrolladas durante esta segunda fase son:

1) Liberación de los servidores físicos migrados, ya que los servicios que se prestaban desde ellos son prestados ya desde máquinas virtuales en la plataforma virtual.
2) Instalación del VMware vSphere 5, siguiendo el procedimiento descrito en el apartado 4.3.
3) Configuración básica de los servidores y su integración en la red Ethernet y en la red de almacenamiento, siguiendo los procedimientos destinados a ellos descritos anteriormente en este capítulo 4.
4) Integración de los servidores físicos, añadiéndolos al clúster de servidores ESXi y realizando las configuraciones restantes de VMware realizadas en el resto de servidores y que han sido descritas anteriormente.

Con la finalización con éxito de este procedimiento, ya se dispone de una arquitectura virtual compuesta por un clúster de 6 servidores físicos ESXi y con todo el pool de recursos que se había descrito en el diseño de la arquitectura virtual.

4.5.5. Supervisión del pool de recursos de CPU y RAM

La capacidad de vRAM disponible y configurada se puede supervisar y gestionar mediante el módulo de gestión de licencias de VMware vCenter Server. De este modo, se han configurado alertas para obtener notificaciones automatizadas por correo cuando el nivel de uso de vRAM supere un nivel especificado de capacidad disponible en el pool. Para ello, se utiliza la pestaña *Reporting* de la opción *Licensing* del panel de administración de VMware vSphere Client.

A continuación, se muestran una serie de imágenes que muestran el pool de recursos del clúster, disponible y en uso, en cuanto a CPU, memoria y almacenamiento. Las imágenes ofrecen información sobre la capacidad total de CPU y memoria del clúster, la capacidad reservada por las máquinas virtuales para operaciones de vSphere HA y la capacidad que queda disponible.

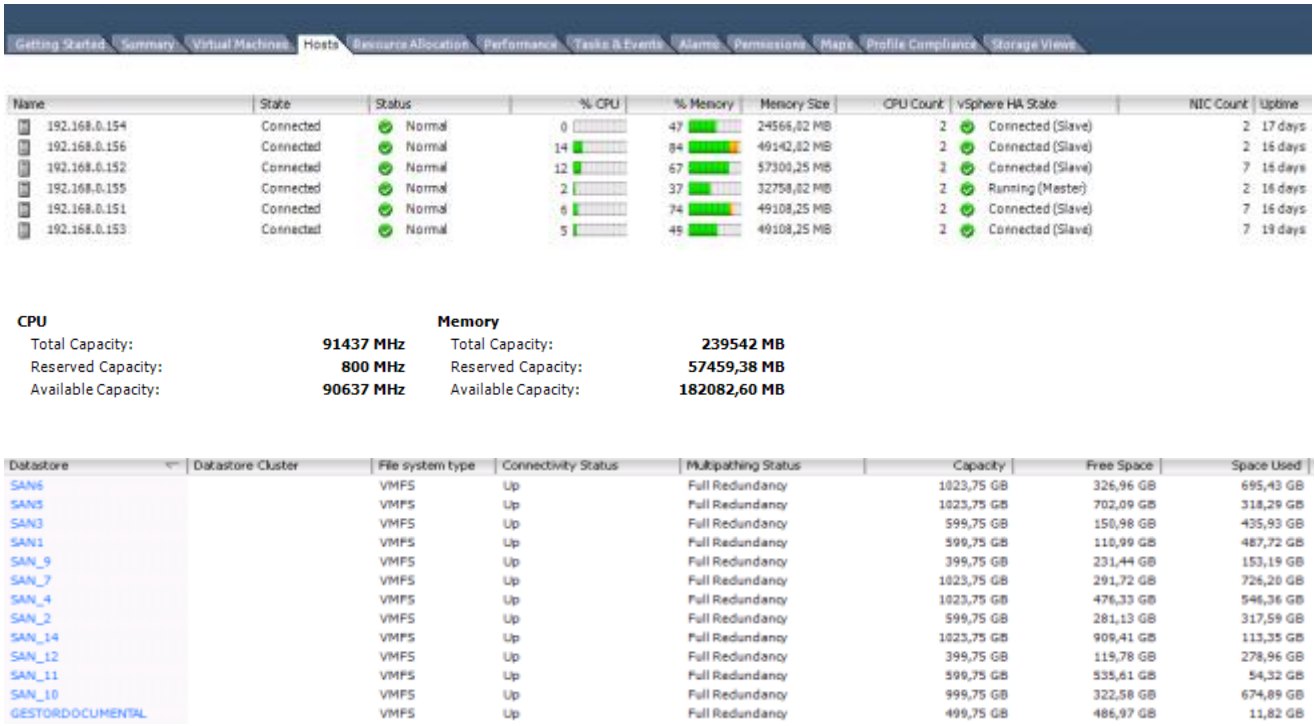


Figura 40: Pool de recursos de la arquitectura virtual.

En la siguiente imagen se muestra un resumen de la configuración disponible en el clúster de la arquitectura virtual configurada en la que puede observarse información detallada sobre las características del clúster:

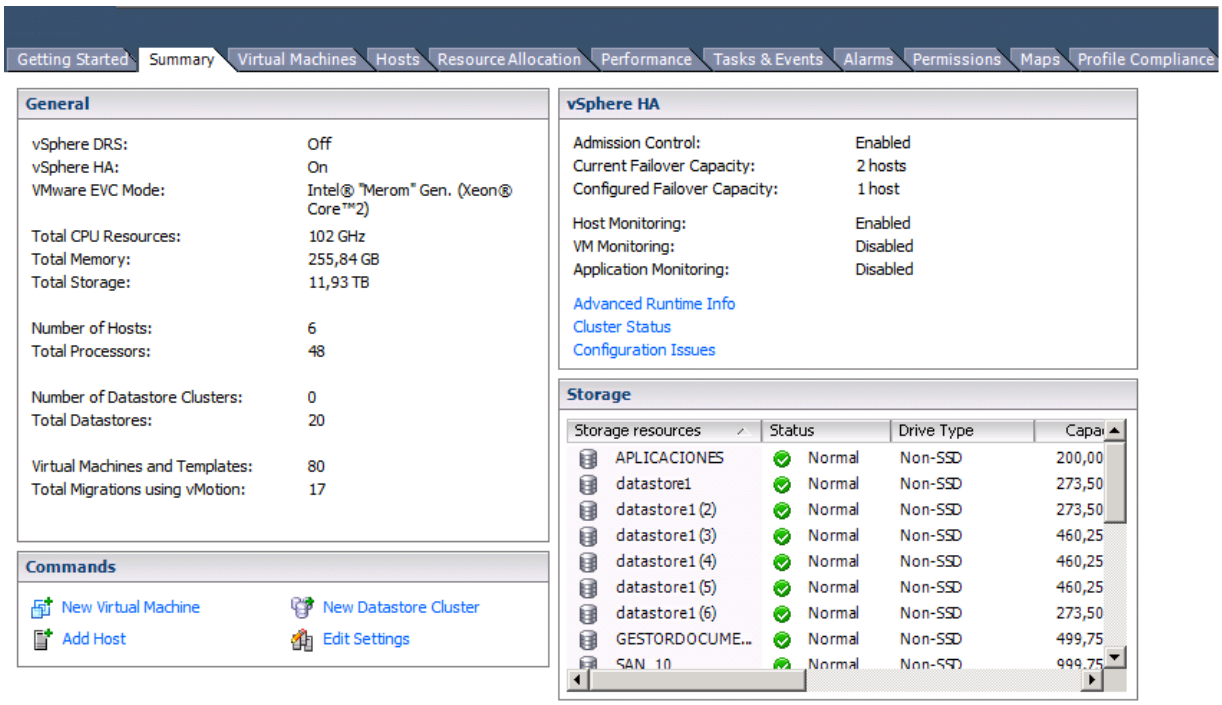


Figura 41: Clúster arquitectura virtual con VMware

El panel de navegación de VMware vSphere Client permite en todo momento ofrecer información detallada de todos sus elementos de inventario a nivel de Datacenter, Cluster, host ESXi y máquina virtual. Dentro de su panel de bienvenida, el vSphere Client dispone del apartado denominado *Inventory* donde ofrece acceso directos a todos los elementos del inventario clasificándolos según su tipo en *Host and Clusters*, *VMs and Templates*, *Datastores and Datastore Clusters* y *Networking*.

4.6. Resumen y conclusiones

En este capítulo se han descrito detalladamente todas las tareas llevadas a cabo para la implantación de la arquitectura virtual basada en VMware.

Tras el diseño y planificación de la misma, se adquirió todo el material necesario para el despliegue de todos los elementos hardware y software. Tras esto, se ha detallado la implantación del hardware sobre la que se sustenta la infraestructura virtual basada en VMware. Es importante resaltar que el orden de implantación descrito es importante porque determinados elementos necesitan de la instalación anterior de otros para su completa instalación y configuración. Otras implantaciones, sin embargo, puede realizarse en paralelo. Así, durante este capítulo se ha detallado el procedimiento de implantación de:

- La red Ethernet física que permite la implantación posterior de la red virtual VMware y la presentación de servicios hacia internet y hacia las redes internas de la empresa.
- El vCenter Server, que permitirá la gestión centraliza de toda la plataforma virtual.
- Los servidores físicos hosts ESXi, que aportan el pool de recursos sobre el que se sustentarán las máquinas virtuales.
- La red SAN Fiber Channel, que permitirá disponer de un almacenamiento compartido entre todos los ESXi, permitiendo alta disponibilidad (vSphere HA, vMotion), redundancia de datos, recuperación de desastres y continuidad de negocio.
- La configuración de la arquitectura virtual utilizando VMware vSphere 5, permitiendo disponer de toda la suite de funcionalidades que nos aporta la licencia VMware vSphere Standard 5.

Al finalizar este capítulo, ya tenemos disponible la plataforma virtual sobre la que podremos crear servidores virtuales para proporcionar los servicios necesarios.

Capítulo 5:

5. Administración y gestión de la plataforma virtual

VMware proporciona toda una suite de productos que permiten la gestión, administración y optimización de la plataforma virtualizada. Sin embargo, como viene siendo habitual, estas funcionalidades avanzadas solo están presentes en las licencias de mayor precio y prestaciones. Por ello, en nuestro caso no contamos con estas funcionalidades que permiten realizar la mayoría de estas tareas de forma automatizada y, para la realización de las mismas, se deben utilizar procedimientos manuales alternativos y herramientas externas.

Es importante resaltar que todas las tareas y procedimientos de administración y gestión deben/pueden realizarse a nivel de clúster de servidores ESXi, a nivel de ESXi y a nivel de máquina virtual. Por último, destacar que, los elementos físicos fuera de la plataforma virtual, como son la red SAN y la red física Ethernet, se gestionan y administran utilizando las herramientas que pone a disposición el fabricante y que fueron descritas durante el procedimiento de implantación del capítulo 4.

5.1. Procedimientos para la administración de la plataforma VMware

En este apartado se van a describir las tareas de gestión y administración que suelen llevarse a cabo para el mantenimiento de la plataforma virtual. Se van a analizar los distintos puntos de administración de la plataforma virtual que incluye vCenter Server mediante conexión a través VMware vSphere Client.

Las tareas básicas de gestión que son llevadas a cabo en un host ESXi son: gestionar máquinas virtuales que se alojan en ese ESXi, gestionar plantillas, desconectar el host del clúster, añadir permisos, gestionar alarmas del clúster o del host ESXi; apagar, reiniciar, encender o poner en modo mantenimiento el host ESXi, generar informes, quitar el host del vCenter Server, etc. La descripción detallada de cómo realizar todas estas tareas puede encontrarse en [1][2][3].

Una vez finalizada la configuración e implantación de una arquitectura virtual basada en VMware, una de las tareas principales será la creación de los servidores virtuales que implementarán los servicios de los diferentes proyectos y la gestión y administración de estos servidores virtuales. Las tareas principales dentro de la gestión de máquinas virtuales que se alojan en los hosts ESXi son:
Creación de máquinas virtuales: Para la creación de una máquina virtual se utiliza el asistente de creación que está disponible al clicar en la vista *Inventario > Host and Cluster* del VMware vCenter Server. Para iniciar el asistente, se clica con el botón derecho en el host ESXi donde se quiere crear la nueva máquina virtual y se selecciona la opción *New Virtual Machine*. Siguiendo las recomendaciones de las referencias [1][3][9] fueron creadas las máquinas virtuales necesarias según se iban implantando los diferentes proyectos a alojar en la plataforma virtual y se iban conociendo las necesidades específicas de estos servidores virtuales.

Creación y utilización de plantillas: VMware vSphere permite la creación de plantillas a partir de una máquina virtual. Una plantilla es una copia maestra de una máquina virtual que se puede utilizar para crear y aprovisionar nuevas máquinas virtuales. Esto es muy útil para que se pueda aprovechar la configuración básica de una máquina virtual, que en nuestro caso denominamos *base*, para desplegar múltiples máquinas virtuales con la configuración *base* a nivel de VMware vSphere y de sistema operativo ya realizada, con el consiguiente ahorro y optimización en el tiempo de despliegue. Se consigue además un aprovisionamiento menos propenso a errores que el aprovisionamiento de servidores físicos. Una plantilla incluye:

- Un sistema operativo huésped.
- Un conjunto de aplicaciones.
- Una configuración que proporciona equivalentes virtuales a los componentes de hardware.

Las plantillas están presentes en el inventario de VMware vSphere Client junto con las máquinas virtuales. Para crear una plantilla existen 2 opciones: clonar una máquina virtual en una plantilla o convertir una máquina virtual en una plantilla. Cuando se usa la opción de menú *Clone to Template* para clonar una máquina virtual en una plantilla, se conserva la máquina virtual original. Cuando se convierte una máquina virtual en una plantilla, *Convert to Template*, la máquina virtual original se sustituye por la plantilla. En nuestro caso, la opción de aprovisionamiento mediante plantilla resulta de gran utilidad en el despliegue de las máquinas virtuales de proyectos enteros que requieren máquinas virtuales con configuración base idénticas y con sistemas operativos Linux. Para desplegar una máquina virtual a partir de una plantilla se selecciona la opción *Deploy Virtual Machine from this Template* que aparece clicando con el botón derecho sobre la plantilla seleccionada.

Clonación de máquinas virtuales: La clonación de máquinas virtuales es otra forma de aprovisionamiento rápido de máquinas virtuales que incluye VMware vSphere. Un clon es una copia exacta de la máquina virtual y puede realizarse con la máquina virtual origen encendida o apagada. En nuestro caso, se utilizó para aprovisionamiento de máquinas que deben tener una configuración idéntica a las que ya existen, como configuraciones redundantes de servidores e incluso para tareas de backups cuando se realizan despliegues de actualizaciones a nivel de aplicaciones o de sistema operativo. Es importante tener en cuenta que al clonar se debe personalizar tanto el nombre de la máquina virtual clonada como las configuraciones del sistema operativo para evitar conflictos software (licencias de sistema operativo) y de red.

Modificación de la configuración de la máquina virtual: En cualquier momento se puede modificar la configuración de la máquina virtual para agregar hardware, eliminar hardware, ajustar opciones de la máquina virtual, controlar la CPU y los recursos de memoria, etc. Todas estas operaciones se pueden realizar con la máquina virtual apagada y algunas de ellas pueden realizarse incluso con la máquina virtual encendida. Esto permitirá ajustar los recursos que utiliza una máquina virtual en todo momento o ajustar opciones avanzadas como cambiar el tipo de aprovisionamiento del disco virtual de la máquina, sincronizar la hora con el servidor NTP del host ESXi que la alberga, opciones de arranque o marcar la prioridad del reinicio de la máquina en el servicio *vSphere HA*. La prioridad de reinicio de máquinas virtuales determina el orden relativo en que se reiniciarán las máquinas virtuales tras un fallo de host. Estos son los valores posibles: *Disable, Low, Medium, High o Use clúster setting*. En nuestro caso fijaremos la prioridad *High* para las máquinas de la red de producción y la red webs, prioridad *Medium* para las máquinas de la red de preproducción y la prioridad *Low* para el resto de máquinas.

Migración de máquinas virtuales: Permiten trasladar una máquina virtual de un host o *datastore* a otro. La migración puede ser:

- Migración en frío: migración de una máquina virtual que está apagada a otro *datastore* compartido y a otro host ESXi.
- Suspendida: migración de una máquina virtual que está suspendida a otro host o datastore.
- VMware vSphere vMotion o migración en caliente: migración de una máquina virtual que está encendida a un host nuevo sin interrupciones ni tiempo de inactividad. Necesita almacenamiento compartido para poder implementarse ya que todo el estado de la máquina virtual (BIOS, CPU, dispositivo, direcciones MAC) se traslada de un host a otro pero los datos siguen almacenados en el mismo datastore.

- Storage vMotion: migrar los archivos de una máquina virtual a un *datastore* diferente mientras la máquina virtual está encendida. Esta característica no se incluye en la licencia vSphere VMware Standard y, para migrar de *datastore* una máquina virtual debemos hacerlo con la máquina virtual apagada.

En nuestro caso, al no disponer de DRS, se utiliza la migración de máquinas virtuales para balancear la carga de los servidores que componen el clúster de la arquitectura virtual y para el manteamiento programado o la actualización de los servidores físicos ESXi, por lo que esta tarea resulta de vital importancia. Para asegurar la correcta configuración del servicio vMotion de VMware vSphere hay que verificar los siguientes aspectos:

- Las máquinas virtuales deben estar contenidas en un almacenamiento compartido al que tengan acceso todos los ESXi del clúster sobre los que se quiere que funcione vMotion.
- Debe existir un grupo de puertos de VMkernel con la característica vMotion activa en cada host ESXi del clúster y utilizar interfaces de red físicas de velocidad Gigabit o superior. El escenario ideal es utilizar interfaces dedicadas, pero también, como en nuestro caso, puede compartirse la interfaz con otro tipo de tráfico.
- El host origen y el host destino deben disponer de vSwitches idénticos y configurados correctamente.
- Los grupos de puertos a los que pertenece la máquina virtual que va a ser migrada deben existir en el vSwitch del host destino de la operación de vMotion.
- Los procesadores de ambos hosts deben ser compatibles. Esto se asegura con la característica Enhanced vMotion Compatibility (EVC) que se configura en la creación del clúster de hosts ESXi.
- La máquina virtual a migrar no debe estar conectada a ningún dispositivo físico disponible únicamente en el host origen (DVD, disquete, etc.)

En la configuración desarrollada en la arquitectura virtual se cumplen todas las características anteriores por lo que la operación de vMotion se desarrolla sin problemas en la misma.

Creación de snapshot de máquinas virtuales: Los snapshots de máquina virtual permiten preservar el estado de una máquina virtual para poder devolverla al mismo estado en reiteradas ocasiones. Son útiles cuando necesitamos volver al mismo estado varias veces, pero no se desea crear múltiples máquinas virtuales. En nuestro caso, se utiliza, por ejemplo, si realizamos algún despliegue de

software, parche o actualización, los snapshots nos permiten revertir estos cambios en caso de que no se realicen de forma correcta y queramos volver al estado anterior.

Eliminación de máquinas virtuales: Se puede eliminar una máquina virtual de dos formas: del inventario (*Remove from Inventory*) y del disco (*Delete from Disk*). Estas opciones están disponibles al clicar con el botón derecho sobre la máquina virtual a eliminar. Al eliminar una máquina virtual del inventario de Vcenter Server, la máquina virtual se borra del registro del host y del de vCenter Server, pero este proceso no elimina la máquina virtual del *datastore*, por lo que sus archivos de almacenamiento siguen estando en la misma ubicación de almacenamiento y la máquina virtual se puede volver a registrar en el explorador de datastores. Cuando se elimina una máquina virtual de un *datastore*, también se elimina de vCenter Server. Todos los archivos de la máquina virtual, incluso el archivo de configuración y los archivos de discos virtuales se eliminan definitivamente del *datastore*.

A continuación, se va a analizar el panel general de administración del vCenter Server. En la pantalla de bienvenida, de la instancia de vCenter Server, se incluye el apartado administración que incluye los siguientes elementos de configuración [3]:

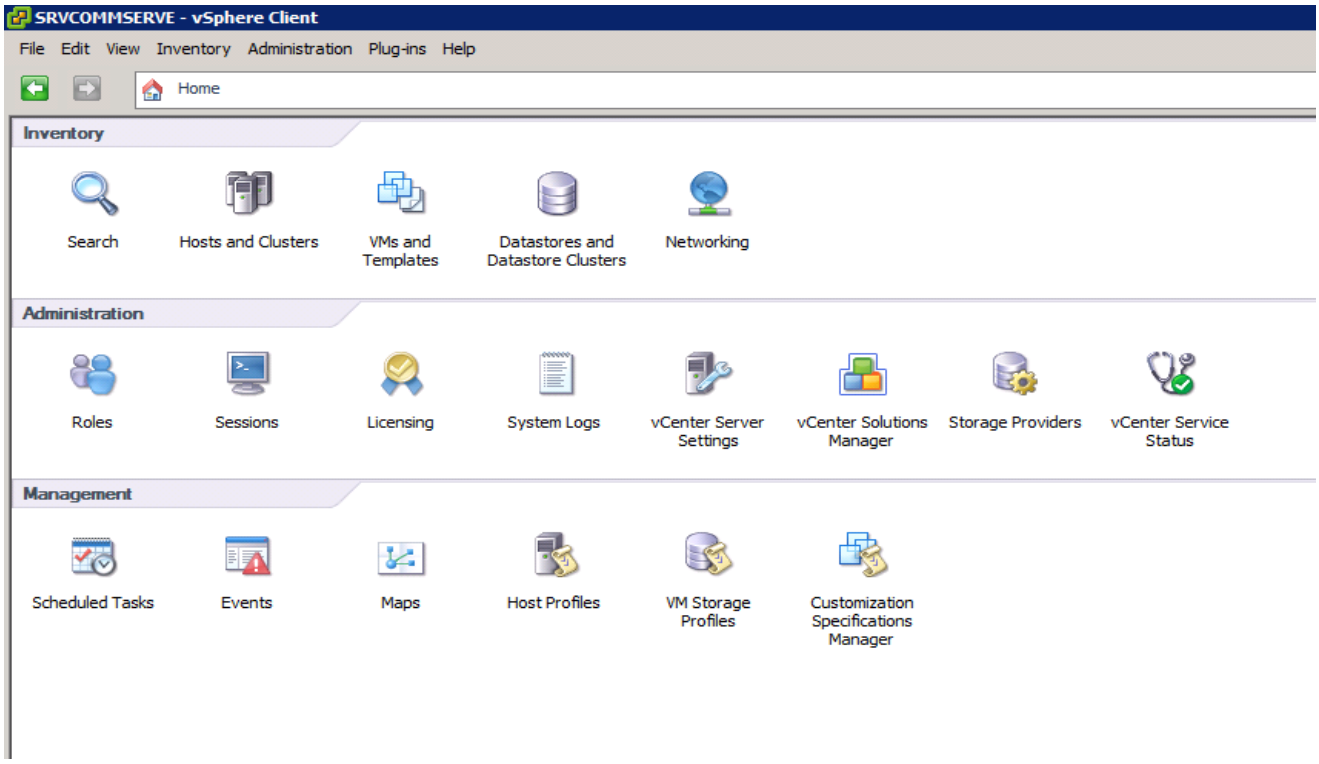


Figura 42: Panel de bienvenida instancia Vcenter Server

Roles: Permite definir diferentes roles de acceso para la gestión de determinadas operaciones. Los usuarios serían encuadrados en estos roles dependiendo de las operaciones a realizar. Se utiliza sobre todo en arquitecturas grandes, con muchos administradores y muchos Vcenter Server. En nuestra compañía, con pocos empleados en TI, una/dos personas engloban todas estas operaciones por lo que únicamente se ha definido el rol de administrador para tener acceso a toda la funcionalidad.

Sessions: Almacena un registro de control acceso al VMware vSphere Client muy útil para auditorías.

Licensing: Proporciona información sobre las licencias contratadas y sus características, los números de serie de las mismas y los servidores ESXi que las están consumiendo.

System Logs: Proporciona un registro de todos los eventos que se realizan sobre la plataforma virtual. El nivel de detalle de registro de estos eventos se puede fijar como veremos más adelante.

vCenter Server Settings: Proporciona un centro de configuración de múltiples características del VMware Vcenter Server, algunas de las cuales ya fueron configuradas durante la instalación:

- *Licensing*: Muestra información de la licencia de VMware vCenter Server instalada.
- *Statistics*: Permite seleccionar el intervalo en el que VMware realiza el almacenamiento de los datos para luego mostrar las gráficas históricas de rendimiento. Además, dispone de una herramienta para calcular el tamaño de la base de datos del vCenter Server en función del número de host disponibles, las máquinas virtuales que se van a gestionar y el número de estadísticas que se desea obtener. Introduciendo los hosts disponibles, que son 6 en nuestra arquitectura virtual, y un número máximo de 100 máquinas virtuales, estimación más del doble de la utilizada en el diseño de la arquitectura, obtenemos un tamaño para la base de datos de 1GB, asumible sin ningún problema.
- *Runtime Settings*: Permite fijar el nombre unívoco del vCenter Server y se utiliza sobre todo en entornos con múltiples Vcenter Server, caso que no se da en nuestra empresa.
- *Active Directory*: Permite fijar parámetros para la integración del Vcenter con un Active Directory. No utilizaremos esta configuración en nuestra empresa ya que el número de administradores que accede al Vcenter Server es pequeño y además solo disponemos de un servidor vCenter Server.
- *Mail*: Permite realizar la configuración de los servidores de correo SMTP para el envío de alarmas a la cuenta del administrador.
- *Logging Options*: permite fijar el nivel de logging entre *None (Disable logging), Error (Error only), Warning (Error and warning), Information (Normal logging), Verbose y Trivia*. En nuestro caso, se fija la opción *Information*, y, en caso de necesidad concreta, aumentaremos el nivel de logging.

- *Database*: Permite fijar el número de conexiones máximas a la base de datos del inventario de Vcenter Server. En nuestro caso, se mantiene el valor por defecto de 50.
- Database Retention Policy: Determina la política de retención de la base de datos para el almacenamiento de tareas y eventos. En nuestro caso tenemos fijado 360 días.
- Advanced Settings: Ofrece un resumen de todas las configuraciones actuales del Vcenter Server.

vCenter Server Status: Muestra información sobre el funcionamiento de todos los componentes, agentes y plugins del Vcenter Server. Hay que vigilar que el estado de funcionamiento sea siempre el óptimo y solucionar cualquier anomalía que pudiera surgir.

Dentro del apartado de gestión del panel de bienvenida del vCenter Server, también se incluyen algunas opciones interesantes de configuración para la gestión y administración de la infraestructura virtual:

Tareas programadas: Muestra el area de tareas programadas dentro del vCenter Server. En esta área se pueden programar la ejecución de tareas períodicas que se ejecutarán sobre la plataforma virtual. Las tareas que pueden ser programadas son: encender o apagar una máquina virtual, clonar una máquina virtual, desplegar una máquina virtual a partir de una plantilla, migrar una máquina virtual con vMotion, crear una máquina virtual, crear un snapshot, añadir un host, cambiar la configuración de encendido de un clúster o cambiar la configuración de recursos para una máquina virtual.

Eventos: Muestra información de todos los eventos que han sido registrados por vCenter Server. Se utiliza para resolver problemas y para tareas de seguridad y auditorías.

Mapas: Proporciona una gran herramienta para rápidas revisiones de los parámetros de la infraestructura virtual. Ofrece mapas topológicos que representan gráficamente las relaciones que existen entre los diferentes objetos del inventario: host y máquinas virtuales, host y red ethernet, host y almacenamiento, máquina virtual y red ethernet, máquina virtual y almacenamiento. Los mapas pueden ser exportados a múltiples formatos.

Otro aspecto importante desde el punto de vista de la gestión y administración de la infraestructura virtual es la configuración de las alarmas:

Alarmas: Una alarma es una notificación que se envía en respuesta a eventos o condiciones seleccionados que ocurren en un objeto del inventario. VMware vSphere dispone de un sistema de alarmas predeterminadas para la mayor parte de objetos del inventario tanto para host como para máquinas virtuales. También es posible definir alarmas personalizadas para máquinas virtuales, host, clústeres, y datastores. Permiten supervisar estados o eventos. Crear una nueva alarma es tarea

sencilla: simplemente clicando con el botón derecho sobre el objeto a monitorizar y seleccionando *Alarm > Add Alarm*. En nuestra plataforma virtual no tenemos actualmente definida ninguna alarma nueva y utilizamos las predefinidas por VMware que abarcan todos los puntos importantes del inventario. Esto es debido a que usamos un sistema de monitorización externo a VMware basado en Nagios y que nos permite monitorizar todos los parámetros de funcionamiento de cada servidor y, sobre todo, el correcto funcionamiento de las aplicaciones.

Sin embargo, el uso de las alertas definidas por defecto en VMware sí que lo utilizamos y la definición de alertas personalizadas resulta muy útil para monitorizar parámetros concretos cuando hay problemas a resolver o quieres prevenirlos. Algunos conceptos interesantes a la hora de definir alarmas en VMware son expuestos a continuación:

- Activador: Toda alarma requiere de un activador, que se encarga de activar la alarma cuando se produce una determinada condición, estado o evento.
- Informes: Se utilizan para definir un intervalo de tolerancia y una frecuencia de activación para los activadores de condición y estado, evitando de este modo restringir más el momento en que el activador reacciona a la condición o el estado y evitando falsas alarmas.
- Acciones: es la operación que se realiza en respuesta al activador. La acción mas usada es enviar una notificación por correo electrónico a uno o varios administradores para que actúen en consecuencia a la alerta recibida. En nuestra arquitectura virtual tenemos configurado la recepción por mail cuando se producen las alertas predefinidas en VMware vSphere configurando el servidor SMTP con los datos del correo de nuestra empresa en el panel *Administración > vCenter Server Settings > Configuración vCenter Server*.

En la siguiente figura se muestra un listado (parcial) de algunas de las alarmas predefinidas por VMware vSphere en los recursos de la plataforma virtual:

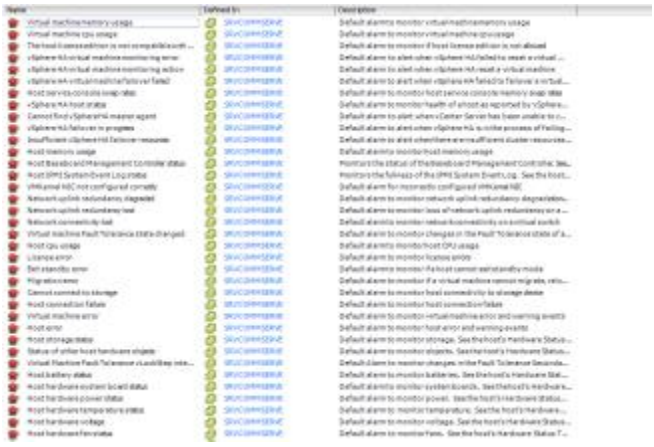


Figura 43: Listado (parcial) de alertas predefinidas

A parte del sistema de alarmas propietario de VMware, en la empresa se utiliza un sistema propietario de alertas basado en Nagios que se complementa con este y que permite monitorizar máquinas virtuales, hosts ESXi, aplicaciones y el estado de los recursos.

Finalmente se termina esta apartado abordando una pestaña que ofrece una información de gran utilidad. VMware ofrece gran cantidad de información de sus objetos de inventario. En el caso concreto de los hosts ESXi, existe una pestaña que muestra información muy útil denominada *Hardware Status*. Esta pestaña de configuración nos permite revisar el estado de los componentes hardware de los servidores hosts ESXi que componen el clúster de la arquitectura virtual. Las alarmas mandarán avisos en caso de producirse alguna anomalía en el hardware. Desde la puesta en producción de la arquitectura virtual han sido necesarias 2 intervenciones para la sustitución de discos del sistema por averías en los mismos que no supusieron interrupciones del servicio ya que están en configuración RAID y, en caso de que el host ESX hubiera interrumpido su funcionamiento, el servicio vMotion hubiera impedido la interrupción del servicio arrancando las máquinas en otros hosts ESXi.

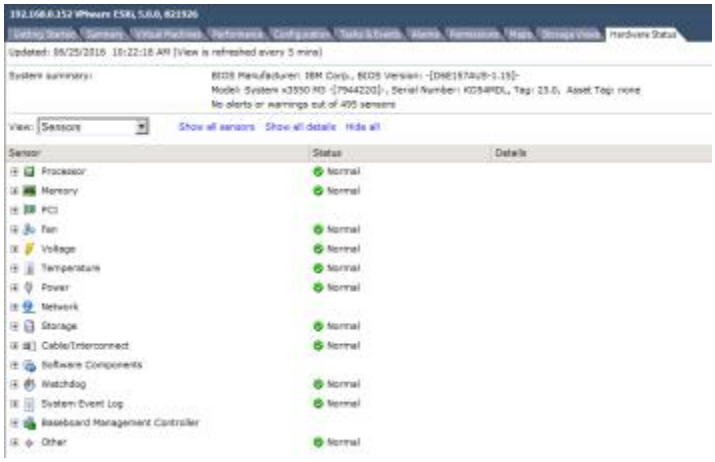


Figura 44: Estado de Hardware de un host ESXi

5.2. Procedimientos para la optimización y gestión de recursos VMWARE

Dado que las máquinas virtuales utilizan simultáneamente los recursos de un host ESXi, necesitan saber qué hacer cuando compiten entre sí por los mismos recursos. Además, hay que tener en cuenta que los recursos son finitos y el número de máquinas virtuales que pueden funcionar de forma

adecuada en un clúster o en un host ESXi también lo es. Para gestionar adecuadamente los recursos, VMware vSphere dispone de distintos mecanismos que podemos utilizar [3][37]:

- Cuota: Habilita una cuota de acceso que especifica la prioridad o importancia relativa para el acceso a un recurso concreto.
- Límite: Evita que una máquina virtual consuma grandes cantidades de un recurso.
- Reserva: Permite que una máquina virtual, cuyo rendimiento no es adecuado o que requiere una cierta cantidad de un recurso para ejecutarse correctamente, disponga de una cantidad garantizada de ese recurso.

Esto permitirá sobreasignar los recursos disponibles mediante una gestión adecuada de los mismos. Cuando se sobreasigna memoria o CPU del host, el objetivo de asignación de una máquina virtual se encuentra entre la reserva y el límite que se haya especificado para la máquina y depende de sus cuotas y de la carga del sistema. VMware vSphere 5 emplea un algoritmo de asignación basado en cuotas para conseguir que todas las máquinas virtuales usen eficazmente los recursos y garantizar un recurso determinado a las máquinas virtuales que más lo necesitan. En la siguiente tabla se muestran los distintos parámetros y funciones que se pueden utilizar para controlar el acceso de la máquina virtual a la CPU, la memoria, el ancho de banda de disco y el ancho de banda de red.

	Managed by VMkernel	Configured by virtual machine creator	Adjustable by administrator
CPU cycles	• Hyperthreading • Load balancing • non-uniform memory access	• VMware vSphere Virtual Symmetric Multiprocessing	• Limit • Reservation • Share allocation
RAM	• Transparent page sharing • vmmemctl • Memory compression • VMkernel swap files for virtual machines	• Available memory	• Limit • Reservation • Share allocation
Disk bandwidth		• Virtual machine file location	• Multipathing • Storage I/O control
Network bandwidth		• NIC teaming	• Traffic shaping • Network I/O control

Figura 45: Parámetros para el control de recursos disponibles (tomada de [37])

Con estas variables podemos realizar una gestión de los recursos que utilizan las máquinas virtuales para permitir dar prioridad de acceso a los recursos a los servicios más importantes y optimizar la utilización de los recursos.

En las licencias de mayores prestaciones, Enterprise y Enterprise Plus, VMware permite funcionalidades adicionales como DRS (vSphere Distributed Resource Scheduler), la creación de

pool de recursos determinados y jerárquicos, que permiten gestionar de forma eficiente y automática en base a políticas prefijadas el pool de recursos disponibles, y herramientas de control de entrada salida en las redes de almacenamiento y ethernet. En nuestro caso, como no disponemos de estas funcionalidades trataremos de suplirlas con una gestión del pool de recursos global manual basada en tablas Excel de control de asignación de recursos a las máquinas virtuales que corren en cada ESXi. Según esto, disponemos de un Excel con todos los recursos disponibles con pestañas a nivel de clúster, a nivel de ESXi y a nivel de máquina virtual y en base a recursos de CPU, almacenamiento, memoria RAM, recursos Ethernet, etc. Para alimentar el Excel utilizamos tanto los datos proporcionados por el VMware vSphere Client, mediante su conexión al vCenter Server, como otras herramientas externas entre las que destaca RVTool que se analizará más adelante al final de este apartado. De este modo, se realiza un control exhaustivo de los recursos disponibles y los recursos consumidos para garantizar en todo momento la existencia de recursos que permitan el funcionamiento óptimo de la plataforma virtual y ayude a planificar una posible escalabilidad de recursos ante demandas programadas o no programadas.

La metodología de ajuste del rendimiento que se sigue en la arquitectura virtual es expuesta a continuación:

1. Evaluar el rendimiento. Para ver con detalle la situación del rendimiento de una máquina virtual debemos usar las herramientas de supervisión del sistema operativo huésped y de vCenter Server. Debemos realizar medidas de referencia antes de realizar los cambios.
2. Identificar el recurso limitador: identificar cual es el recurso del que más depende la máquina virtual. Ese será el recurso que con más probabilidad afectará al rendimiento de la máquina virtual en caso de que esté limitada por él.
3. Hacer disponible más recursos: proporcionando más recursos a la máquina virtual o reduciendo los recursos de otras máquinas virtuales.
4. Tras poner a disposición de la máquina virtual más cantidad del recurso limitante, tomar otra medida de referencia y registrar los cambios.

A continuación se va a analizar con mayor detalle la optimización/métrica de cada recurso:

Almacenamiento

Para un mejor aprovechamiento del espacio de almacenamiento, se utilizan discos virtuales con aprovisionamiento ligero para las máquinas virtuales, lo que nos permite aprovechar al máximo la capacidad de los datastores. Con esto, tenemos *datastores* con sobreasignación ya que el espacio total de aprovisionamiento de discos de aprovisionamiento ligero es mayor que el tamaño del datastore.

Sin embargo, una gestión y control exhaustivos del almacenamiento en cada momento permite desarrollar sin problemas esta política de aprovechamiento y optimización del espacio en disco. Para ello, utilizamos un Excel de control de recursos de almacenamiento y utilizamos las alertas de ocupación de disco que nos proporcionan tanto la cabina de almacenamiento como VMware vSphere Client. Las alertas nos avisan de cuantos discos del *datastore* están sobreasignados o cuanto espacio de disco está usando una máquina virtual. También usamos los informes de almacenamiento para ver el uso de espacio en disco, utilizando por ejemplo el informe *Show all Datastores* de la pestaña *Storage Views* que ya fue mostrado en la figura 40.

Para solucionar problemas de espacio en los datastores y equilibrar la distribución de las máquinas virtuales en los propios datastores se utiliza VMware vSphere vMotion para migrar máquinas virtuales entre datastores. Al no disponer del VMware vSphere Datastore VMotion tenemos que realizar las migraciones de máquinas virtuales entre datastores con las máquinas apagadas. Otra tarea que realizamos para gestionar el uso de espacio es la de aumentar dinámicamente el tamaño del datastore cuando sea necesario. Otras tareas que realizamos para optimizar el uso de los *datastores* son expuestas a continuación:

- Definir "Tiers" o prioridades de LUN: Es básico definir el rendimiento que cada aplicación requiere, y tener en base al rendimiento requerido distintos grupos de LUN con características específicas de rendimiento, capacidad, etc.
- Limitar el número de máquinas virtuales por *datastore*: Una buena práctica es limitar el número de máquinas virtuales por datastores a un máximo de 15 máquinas virtuales.
- Crear un *datastore* específico para imágenes ISO: Con esto logramos una mejor administración y una mejor velocidad en el momento de instalaciones.
- Crear un *datastore* específico para plantillas: una mejor administración de la librería de máquinas virtuales.
- *Multipathing*: usar el *multipathing* que te proporciona la configuración del almacenamiento SAN FC que se realizó mediante el uso de la política Fixed utilizando las 2 controladoras de la cabina en activo-activo.

Memoria RAM

Una característica importante a considerar en entornos VMware VSphere es la sobreasignación de memoria de la máquina virtual que permite disponer de una cantidad de memoria asignada a las máquinas virtuales superior a la cantidad de memoria física instalada en un host ESXi. Mediante esto, el VMkernel se asegura de que el sistema operativo huésped utiliza al máximo la memoria física del

host. Cuando algunas máquinas virtuales tienen una carga ligera, no utilizan la totalidad de la memoria que tienen asignada, por lo que la mayor parte del tiempo la memoria está inactiva. La sobreasignación permite que VMkernel reclame la memoria, tomando la que no utilizan las máquinas virtuales inactivas para entregárselas a otras máquinas virtuales que la van a utilizar de forma activa.
VMkernel utiliza varias técnicas para reclamar la memoria de un host VMware vSphere ESXi que merecen ser mencionadas: *Transparent page sharing*, *Ballooning*, swap, swap a SSD y comprensión de memoria. Estas técnicas han sido analizadas en profundidad en [3][37].
Para comprobar si los valores de funcionamiento de la memoria RAM de una máquina virtual dentro de un host ESXi son los correctos, debemos verificar y analizar una serie de métricas que son mostradas en el vCenter Server, en la vista inventario, en la pestaña *Resource allocation* de la máquina virtual

- *Private*: La cantidad de memoria almacenada en la memoria del host físico para esta máquina virtual.
- *Shared*: La cantidad de memoria compartida entre varias máquinas virtuales con Transparent Page Sharing.
- *Swapped*: La memoria del host se swappea dentro de un archivo dentro del directorio de la VM para liberar la memoria del host.
- Compressed: Memoria que haya sido comprimida por el VMkernel para liberar espacio proporcionando mejor rendimiento que el swapping.
- *Balloned*: Memoria reclamada desde sistema huésped por el driver balloning.
- *Unaccessed*: Memoria que no es utilizada ni tocada por la máquina virtual.
- Active: La memoria del sistema Huésped que está en buen estado usado por la máquina virtual.
- Consumed: La memoria del host que se asigna a la máquina virtual.

Si se tiene mucha memoria en los estados de reclamación por parte del sistema huésped, entonces hay que revisar la memoria de la máquina virtual y la memoria general de hosts porque estamos llegando al límite de la sobreasignación. A nivel de host podemos analizar los valores de la memoria utilizando gráficos como veremos a continuación.
Para evitar problemas de funcionamiento es importante la monitorización y control de estos parámetros y llevar siempre un control general mediante hojas Excel y herramientas como Rvtool*

* La información sobre esta herramienta se encuentra en http://www.robware.net/

para conocer en todo momento la memoria física de la que dispone el host, la memoria asignada a las máquinas virtuales y la utilización de la misma.

CPU

A nivel de CPU existen ciertas medidas para determinar el rendimiento de un host o de una máquina virtual, y para hacer uso eficiente de los recursos manteniendo las cargas de trabajo. En cuanto al uso de CPU de una máquina virtual, se deberán añadir vCPU adicionales cuando el uso medio de CPU se mantenga en niveles elevados. A nivel de host el parámetro a controlar es el *CPU Ready*, que determina el tiempo que una máquina virtual está esperando para obtener vCPU disponibles que necesita. Las mejores prácticas [38] determinan que un valor óptimo es el situado por debajo del 5%, un valor malo se sitúa entre el 5% y el 10% y un valor es considerado muy malo por encima del 10%. Si tenemos un host cuyo CPU Ready se sitúa por encima del 5%, la solución es mover máquinas virtuales a otros hosts ESXi utilizando vMotion para repartir la carga de CPU en el clúster o repasar las vCPUs asignadas a las máquinas virtuales para tratar liberar recursos de CPU. Los parámetros de uso de CPU medio de las máquinas virtuales y de CPU Ready de los hosts se obtienen mediante la obtención de gráficos utilizando las herramientas destinadas a ello del vCenter Server que veremos a continuación.

Otro parámetro que ayuda a optimizar la CPU es el hyperthreading, que permite que un núcleo ejecute dos subprocesos o conjuntos de instrucciones a la vez. Sin embargo, las CPUs físicas de los servidores físicos de la infraestructura virtual no disponen de esta característica. Es una tecnología propietaria de Intel que permite optimizar el uso de los Procesadores pudiendo utilizar múltiples procesos de forma paralela

Red Ethernet

Finalmente, en cuanto a la red Ethernet, se pueden analizar múltiples parámetros utilizando los gráficos de rendimiento del vCenter Server para ver posibles cuellos de botellas en las redes virtuales desplegadas. Entre ellos destacan: Tasa de datos recibida/transmitida, paquetes transmitidos, paquetes recibidos, paquetes perdidos, etc.

5.2.1. Gráficos de rendimiento del vCenter Server

En este apartado se van a analizar los gráficos de rendimiento de vCenter Server [1][3][39]:

La pestaña *Perfomance*, del vCenter Server, permite supervisar el rendimiento de un clúster, host o máquina virtual en tiempo real o durante un período de tiempo. Los gráficos generales de rendimiento muestran las estadísticas que VMware considera más útiles para supervisar el rendimiento y diagnosticar problemas. Se permiten obtener gráficos de los contadores más comunes para mediciones de CPU, disco, memoria y redes permitiéndonos analizar el rendimiento de host o máquinas virtuales y determinar si una máquina virtual esta limitada por un recurso: CPU, memoria RAM, disco y red. Los gráficos de rendimiento proporcionan una rápida representación visual del funcionamiento del host o la máquina virtual, según el recurso a analizar y permiten descubrir problemas de rendimiento, supervisar tendencias de uso, planificar la capacidad y determinar los recursos que se deben aumentar y disminuir en los hosts y en las máquinas virtuales. Los gráficos se pueden personalizar con distintos objetos y contadores para obtener los datos buscados y pueden mostrarse apilados para comparar rendimientos o en forma lineal para analizar un recurso de forma individual. En cuanto a los intervalos temporales, vCenter Server usa 5 intervalos de recopilación: tiempo real, día, semana, mes y año.

Las gráficas a nivel de clúster y a nivel de host permiten determinar durante lo primeros meses de vida de la plataforma virtual si el diseño de la arquitectura se realizó de forma correcta. La gran variedad de posibilidades que ofrecen los gráficos en cuanto a recursos a mostrar, intervalos de muestreo o medidas mostradas hacen de esta una gran herramienta para el análisis de problemas de recursos a nivel de clúster, hosts y de máquinas virtuales que permiten optimizar el funcionamiento de la arquitectura virtual y de los servicios en particular. Además, estas herramientas permiten mostrar gráficos superpuestos que permiten comparar parámetros de máquinas virtuales entre sí y con el host ESXi. La mayoría de los análisis que se han realizado en la arquitectura virtual han sido a nivel de máquina virtual para tratar de mejorar la prestación de cualquier servicio. Para ello, se utilizan gráficas similares a las anteriores, pero con intervalos temporales pequeños con el fin de analizar con más detalle la evolución de los recursos. Se debe comprobar si:

- La máquina virtual está limitada por CPU. Esto se produce si el uso de CPU de la máquina virtual es muy alto durante un período de tiempo. Si hay más de una máquina virtual limitada por la CPU, el indicador clave es el tiempo de CPU *Ready*.
- La máquina virtual está limitada por la memoria. Los parámetros a monitorizar son swap y balloning. Cuando se produce este hecho en la máquina virtual, la actividad de balloning es

elevada de forma continuada y el sistema operativo huésped comienza a paginar. Si hay varias máquinas virtuales limitadas por la memoria, se observa además que la máquina virtual está haciendo intercambio con el VMkernel, produciéndose una situación grave que indica que la memoria del host esta sobreasignada. Para solucionar esta situación se puede:

- Reducir el espacio de memoria en la máquina virtual y corregir el tamaño de la caché si es demasiado grande. Esto libera memoria para otras máquinas virtuales.
- Migrar una o varias máquinas virtuales a otro host dentro del clúster.
- Añadir más memoria física al host.

- La máquina virtual está limitada por el disco. Los gráficos pueden informar sobre el rendimiento de una máquina virtual al permitir supervisar el rendimiento y latencia de un *datastore*, un adaptador de almacenamiento o una ruta de almacenamiento. Una forma fiable de comprobar si el entorno vSphere está experimentando problemas de disco consiste en supervisar los contadores de latencia de disco. Para supervisar el rendimiento hay que observar los contadores de tasa de lectura y tasa de escritura. Para supervisar la latencia se observan los contadores de latencia de lectura y latencia de escritura. Otros contadores importantes que determinan problemas de rendimiento de disco son:
  - Latencia de comando del kernel: tiempo medio empleado por el VMkernel para procesar un comando SCSI. Un número alto en este contador, entre 2 a 3 milisegundos, puede significar:
    - Que la cabina tenga un exceso de trabajo
    - O que el servidor ESX/ESXi tenga un exceso de trabajo.
  - Latencia de comando del dispositivo físico: Mide el tiempo medio que el dispositivo físico (disco) necesita para completar un comando SCSI. Un número alto en este contador (depende de la cabina, pero, en general, este valor está entre 15 y 20 milisegundos), puede significar dos cosas:
    - O la cabina va muy lenta.
    - O la cabina tiene un exceso de trabajo.

- La máquina virtual está limitada por red. El origen de los problemas de red suele ser la saturación de una conexión de red entre el cliente y el servidor. Para comprobar si se pierden paquetes de red se utilizan los gráficos de rendimientos para examinar los valores *droppedTX*

y *droppedRX* del contador de red de una máquina virtual y pueden realizarse prueba de transferencia de ficheros grandes para determinar el rendimiento de la transmisión y detectar posibles problemas. En nuestro caso analizamos las graficas de rendimientos con los valores *droppedTX* y *droppedRX* y mostraban todos los valores a 0, determinando su funcionamiento óptimo.

A continuación, vamos a mostrar algunos gráficos del host ESX2 (192.168.0.152) donde se analizan este tipo de limitaciones de recursos. A continuación se muestra un gráfico para analizar la CPU:

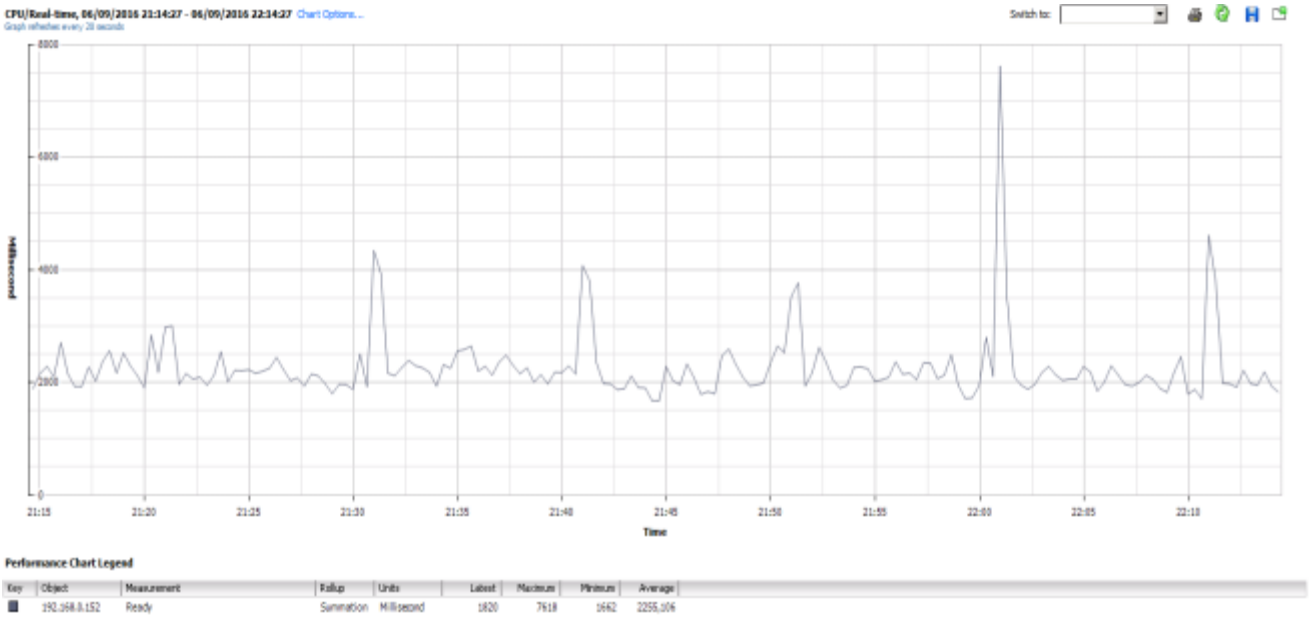


Figura 46: CPU Ready para el ESX2

En la gráfica anterior se muestra el valor CPU Ready del host ESX2 para un espacio temporal de una hora. Como hemos comentado esta métrica es realmente importante para determinar si estamos teniendo problemas de rendimiento de CPU. El valor de la gráfica está en milisegundo y podemos pasarlos a porcentaje teniendo en cuenta el tiempo de muestreo de la gráfica, 20 segundos en la gráfica de real time. Según esto, utilizamos la siguiente fórmula de conversión:

(x ms / 20.000 ms) * 100 = %rdy
Según la cual: 1% = 200ms, 5% = 1000ms, 10% = 2000ms o 100%=20000

Con la conversión anterior, el valor máximo, que se sitúa en 7618 milisegundos correspondería a un porcentaje de 38,79 para las 8 vCPU de las que dispone el host ESX2 y de 4,76% por cada vCPU. Por

lo tanto, en el caso peor el CPU Ready se mantiene en un valor óptimo, al estar por debajo del 5%, y el uso de CPU en el host ESX2 es adecuado y correcto. Además, el valor promedio se sitúa en torno al 1,4% para cada vCPU, lo que indica que este hosts puede soportar muchos más recursos de vCPUs.

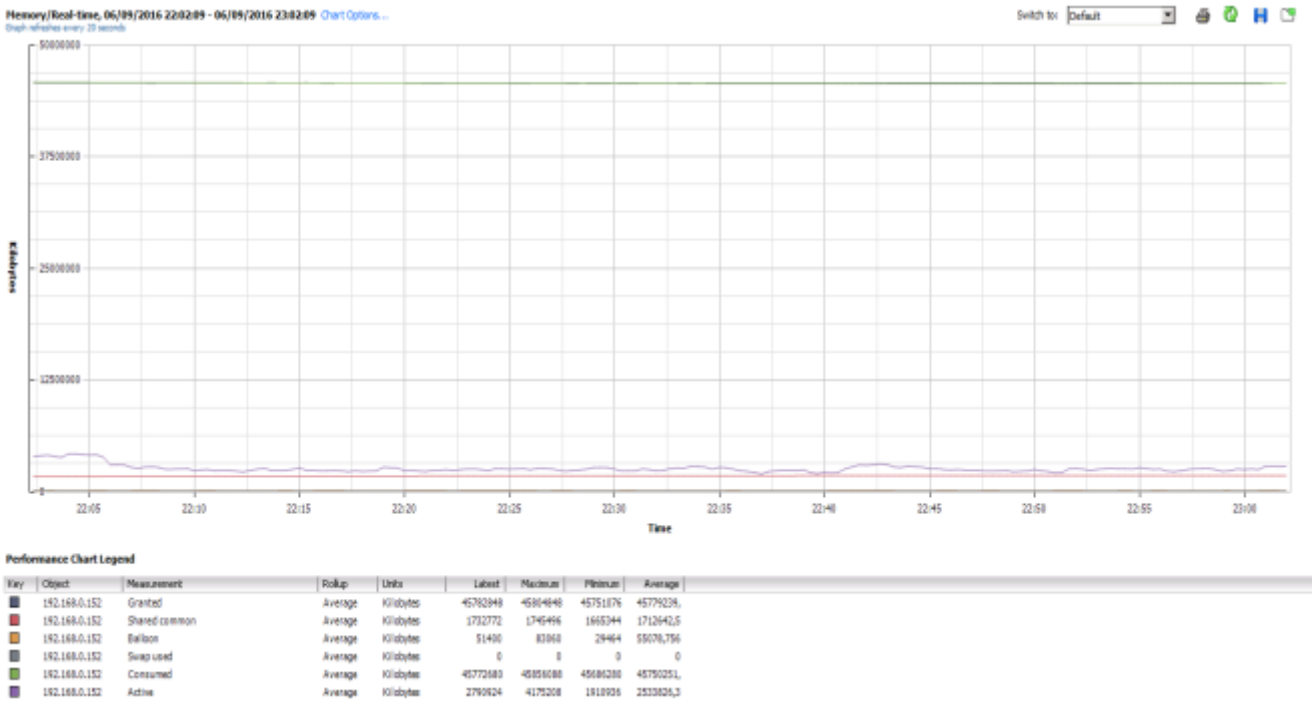


Figura 47: Uso de memoria RAM del ESX2

En la gráfica anterior se muestra información sobre la situación de la utilización de la memoria RAM en el host ESX2. En ella pueden verse los valores que alcanzan las distintas métricas utilizadas para el análisis de la memoria RAM en VMware y puede verse que los principales parámetros de reclamación de memoria que permiten la sobreasignación de la misma, *Ballon* o *Swap*, adquieren valores muy bajos, lo que indica que la distribución de memoria física del host, hacia las máquinas virtuales que funcionan en él, se encuentra en valores óptimos y lejos del máximo, al no estar realizándose apenas reclamación de memoria por parte del driver de balloning de las máquinas virtuales.

En las siguientes gráficas pueden verse la latencia de comando del kernel y la latencia de comando de dispositivo para el host ESX2. En ellas puede verse como ambos valores analizados están en unos valores normales. Si hubiera algún valor que se saliera del rango óptimo de funcionamiento, analizaríamos la LUN determinada donde se están produciendo problemas seleccionando el color para identificarla. Posteriormente analizaríamos las máquinas virtuales que están utilizando dicha LUN y el tráfico que están generando para identificar cual es la que está provocando el problema. Otro procedimiento sería ir moviendo una a una cada máquina virtual a otra LUN y verificar cual es la que está provocando este fallo.

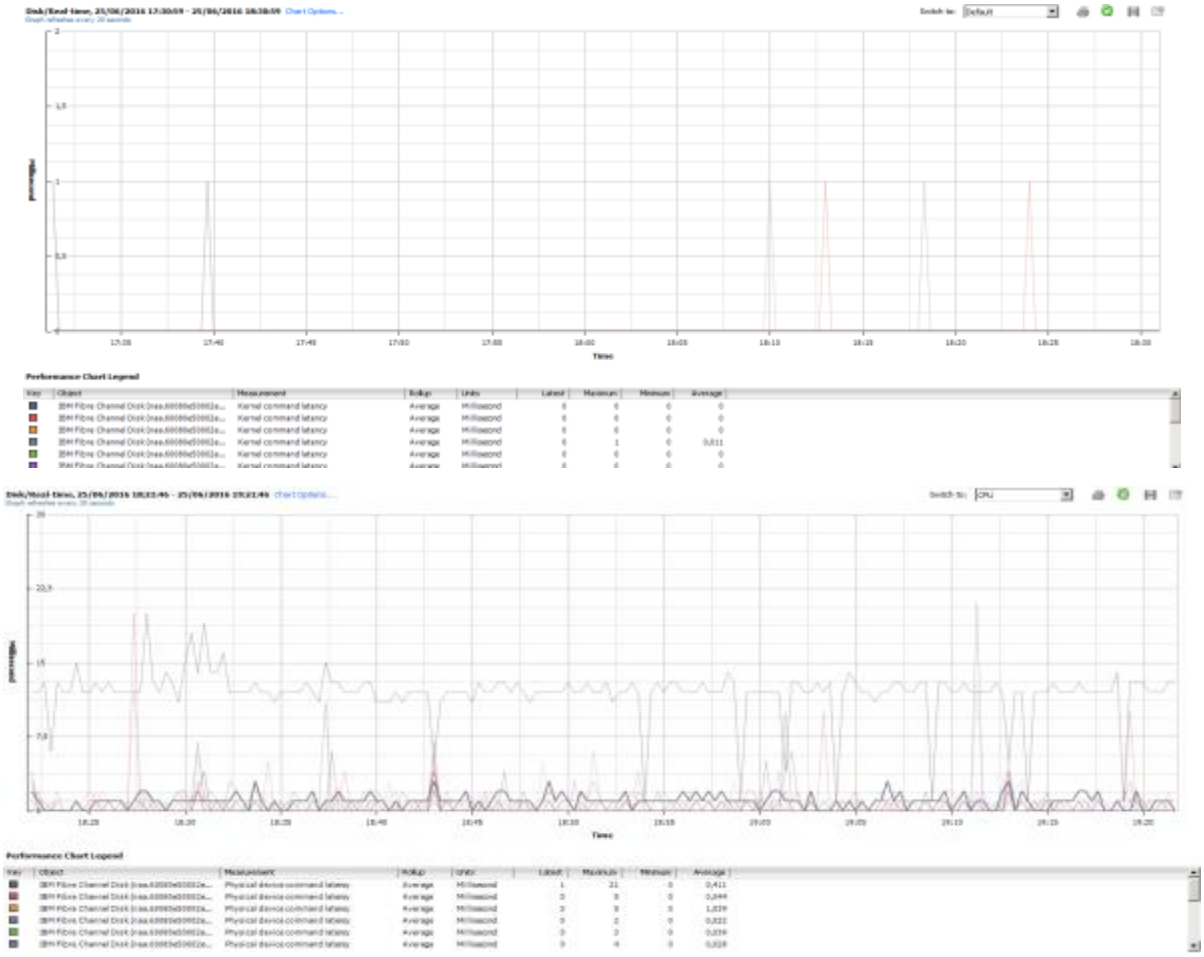


Figura 48: Latencia de comando del kernel y latencia de comando del dispositivo físico

Por último, cabe mencionar y presentar una herramienta que también se utiliza mucho en la gestión de la infraestructura virtual y que se denomina *Rvtools*. Se trata de una herramienta libre basada en .NET y que permite ofrecer información detallada sobre todos los elementos de nuestra arquitectura virtual: ESXi, máquinas virtuales, CPU, memoria RAM, almacenamiento, snapshots, VMware Tools, clúster, HBAs, NICS, Switches, grupos de puertos, datastores, etc. De este modo, nos permite visualizar, analizar y gestionar los recursos y ayuda a la resolución de incidencias y optimización. En nuestro caso la instalación es en el servidor físico donde está instalado el Vcenter y lo conectamos a nuestra plataforma virtual. En la siguiente imagen se muestra la información de las interfaces virtuales que ofrece Rvtool:

Figura 49: Herramienta RVtools sobre el la arquitectura virtual

Como puede verse se trata de una herramienta muy potente que ofrece gran cantidad de información y resulta de gran ayuda en la administración de la plataforma.

5.3. Herramientas complementarias de administración y gestión

Además de las interfaces de usuario gráficas, proporcionadas mediante la conexión a la instancia de vCenter Server mediante el VMware vSphere Client o VMware vShere Web Client, se puede gestionar toda la plataforma virtual a través de herramientas y aplicaciones complementarias que utilizan línea de comandos. Para realizar tareas de gestión desde una línea de comandos remota podemos utilizar [39][40]:

- VMware vSphere Command-Line Interface (vCLI): Se trata de un conjunto de comandos activados desde un sistema Linux o Windows remoto y ejecutados en un host ESXi.
- VMware vSphere Management Assistant (VMA): Se trata de una plataforma para la ejecución de distintos conjuntos de herramientas:
    - vCLI
    - VMware vSphere SDK para perl.
    - VMware vSphere API

  - VMware VSphere PowerCLI: Se trata de una herramienta de automatización para administrar un entorno vSphere (Windows Powershell)
  - VMware Tools.

  Los comandos más frecuentes utilizados en vMA son: esxcli, resxtop, svMotion, vicfg-*, esxcfg-*, vifs, vihostupdate, vmkfstools, VMware-cmd.

- ESXi Shell: Permite acceder al ESXi desde la consola local de usuario (DCUI) o remotamente utilizando SSH (por defecto viene activado y no es recomendable si el acceso no es a nivel LAN).

Todas estas herramientas permiten realizar tareas de administración sobre los ESXi y máquinas virtuales desde líneas de comandos. Permiten realizar toda la funcionalidad que proporciona VMware VSphere Client y proporciona funcionalidades avanzadas. Además, permite desplegar un conjunto de comandos, scripts, sobre *datacenter*, clúster de ESXi y máquinas virtuales. Sobre todo, se utilizan en entornos virtuales con grandes cantidades de host ESXi, máquinas virtuales y varios Vcenter Server.
En nuestro caso hemos utilizado en mayor medida las herramientas que proporciona el propio VMware vSphere Client pero cada vez se realizan más tareas de mantenimiento, administración y optimización utilizando estas herramientas.

5.4. Resumen y conclusiones

En este capítulo se han descrito detalladamente todas las tareas y procedimientos que permiten realizar la configuración avanzada de VMware vSphere 5 así como las tareas de gestión y administración habituales para el mantenimiento de la plataforma virtual. Por ello, se han descrito las tareas básicas de gestión que son llevadas a cabo a nivel host ESXi o máquina virtual. Además, se han analizado las funcionalidades que permite el panel de gestión y administración de la instancia del vCenter Server a través del vSphere Client.

Seguidamente se han analizado los procedimientos que permiten la gestión y optimización del pool de recursos que proporciona el clúster de hosts ESXi a los servidores virtuales que funcionan en ellos. Estos procedimientos permiten ajustar el rendimiento, inventariar la asignación de recursos, analizar la forma de uso y el estado de utilización de cada uno de los recursos importantes: CPU, memoria RAM, almacenamiento en disco, red Ethernet; analizando aquellos parámetros importantes en cada recursos que permiten determinar si el funcionamiento de la plataforma es el óptimo. Para ello, se han utilizado los gráficos de rendimiento del vCenter Server y se han mostrado ejemplos de

medidas y análisis de parámetros importantes y habituales para la optimización del funcionamiento a nivel de ESXi y de máquina virtual.

Finalmente se han enumerado herramientas alternativas y complementarias a las proporcionadas del vCenter Server que permiten mejorar, complementar, y automatizar los procedimientos de gestión y administración y, en consecuencia, el funcionamiento general de la plataforma virtual y los servicios que presta.

Capítulo 6:

6. Copias de seguridad, recuperación de desastres y continuidad de negocio

En este capítulo se van a describir los procedimientos y configuraciones llevados a cabo para la replicación y redundancia del centro de datos, activo más importante de la empresa y que asegura la continuidad de negocio. Las políticas para la replicación de los datos se basan en 2 procedimientos independientes y complementarios:

- Realización de copias de seguridad de la información que reside en la arquitectura virtual. Esto permite una rápida recuperación de cualquier información concreta durante el período de retención de la información, guardando múltiples versiones de la información que pueden ser recuperadas y utilizadas en cualquier momento.
- Clonación del centro de datos: Esto permite disponer de una copia exacta de los datos de la cabina principal y en la misma configuración permitiendo la recuperación ante desastres del centro de datos en el menor tiempo posible. De este modo, con este y otros procedimientos complementarios se asegura la continuidad de negocio.

6.1. Sistemas de Copias de Seguridad

A lo largo del tiempo, nuestro entorno de VMware vSphere podría sufrir cambios en la configuración del hardware o del software. Además, los datos de las aplicaciones cambian constantemente. Por este motivo, desde el punto de vista de la gestión, es importante realizar copias de seguridad regulares del entorno de VMware vSphere. La realización de copias de seguridad, en nuestro caso diarias, permite disponer de múltiples imágenes temporales de las máquinas virtuales con las que hacer frente a posibles incidencias relacionadas con la pérdida de datos que pudieran surgir.

Gracias a su flexibilidad, las arquitecturas virtuales tienen muchas ventajas en cuanto a las estrategias de backup. Estas ventajas ofrecen un ahorro de tiempo y dinero, además de introducir en el centro de datos nuevas tecnologías que no existen para las arquitecturas físicas:

- Las máquinas virtuales siempre ven el mismo conjunto de hardware virtual, sea cual sea el hardware instalado en el servidor físico y esto facilita las recuperaciones directamente en el hardware. Los servidores físicos necesitan procesos distintos para crear restauraciones directamente en el hardware y a nivel de archivos.
- Las máquinas virtuales solo necesitan un backup a nivel de imagen, que puede servir tanto para la restauración directamente en el hardware como para la restauración a nivel de archivos.
- Las máquinas virtuales no necesitan tener instalado un agente de backup, porque las soluciones de backup creadas para las arquitecturas virtuales pueden acceder directamente a los *datastores* de VMware vSphere. El acceso directo al *datastore* permite descargar los procesos de backup en un servidor distinto del host en el que se ejecutan las máquinas virtuales; esto también significa que los backup no consumen ancho de banda de red.

En el mercado, existían en ese momento múltiples soluciones profesionales para la realización de las copias de seguridad de nuestro centro de datos. Dentro del elenco de soluciones disponibles se seleccionó la solución ofrecida por Simpana Commvault[41], incluso por delante de la solución que comercializa VMware. Las razones que llevaron a esa elección fueron:

- Se trataba de una solución ofrecida por una empresa dedicada única y exclusivamente a soluciones de copias de seguridad y replicación de centro de datos.
- Los premios y buenas críticas recibidos por esta solución como mejor producto de backup, justo cuando se estaba sondeando el mercado.
- Recomendaciones de calidad que recibimos de algunos de nuestros proveedores que ya conocían y usaban la solución en sus empresas.
- La solución se ajustaba económicamente al presupuesto disponible.

Por estos motivos, para la realización de las copias de seguridad de nuestro centro de datos se decide la contratación del software profesional Simpana Commvault. El software Simpana Commvault es una suite de archivado y backup que realiza tareas de replicación y tareas de almacenado de ficheros para su archivado. Para la instalación de la citada solución, se contrata una empresa externa especializada que se encargó de la instalación y configuración inicial del producto. La instalación del producto se realizó en el servidor físico sobre el que ya estaba instalado el vCenter Server y que, como ya se había anunciado en capítulos anteriores, actuaría como núcleo central para la administración de las copias de seguridad. La instalación de software Simpana Commvault se realiza utilizando una base de datos SQL Server Enterprise.

Para la gestión del producto se utiliza un cliente denominado *Commcell Console*. Se trata de una consola que permite la realización de las tareas de gestión, configuración avanzada y administración, dentro del producto Simpana Commvault que se reflejan directamente sobre las políticas y procedimientos de copias de seguridad. Todas estas tareas son realizadas directamente por mi empresa a través de mi persona. A continuación, se van a describir los elementos más importantes del proceso para la realización de las copias de seguridad [41]:

- *Media Agent*: es el encargado de copiar los objetos del vCenter Server, máquinas virtuales encendidas o apagadas, y plantillas, en las librerías de almacenamiento.
- Políticas de almacenamiento: son políticas que se utilizan para configurar dónde se hacen las copias. En estas políticas, se indica el camino que van a seguir los datos desde el origen hacia la librería de almacenamiento destino. También se fija la retención temporal de los datos en la librería de almacenamiento. Cuando se cumple el ciclo de retención fijado, existen tareas de borrado propias de Simpana Commvault que se encargan de la eliminación de la información más antigua que el período fijado. Las políticas de almacenamiento más destacadas son:
    - Deduplicación: se trata de una política intrínseca que ya viene configurada en el producto. Esta técnica de respaldo elimina los datos redundantes almacenados, guardando una única copia idéntica de los datos, y reemplazando las copias redundantes por indicadores que apuntan a esa única copia. En cada copia de seguridad, junto con los datos se guardan los índices para localizar dichos datos. Estos índices se guardan mediante esta política de almacenamiento. La política se basa en el almacenamiento de la base de datos con la información de deduplicación.
    - Recuperación de desastres (DR): es la política de almacenamiento dedicada a las copias de seguridad de la base de datos SQL sobre la que está implementada la instalación y las configuraciones avanzadas del Simpana Commvault. Se utiliza para la recuperación de desastres del propio producto. No hay política de programación dedicada para esta copia ya que no se trata de un backup como tal sino que es una tarea administrativa de la plataforma Commvault.
    - Backups de datos: es la política que se utiliza exclusivamente para la copia de las máquinas virtuales y plantillas almacenadas en las librerías de almacenamiento destinadas a ello.
- Políticas de programación: son las políticas que se utilizan para planificar temporalmente cuándo se realizan las copias de seguridad. En estas políticas se decide cuándo se van a ejecutar las políticas de almacenamiento y el tipo de copia que se va a realizar: completa,

incremental o diferencial. Siempre las políticas de almacenamiento van a llevar asociada una política de programación para poder gestionar de forma automática los backups. También se pueden ejecutar tareas de forma manual cuando se requiera. En la siguiente tabla se muestra la programación de las distintas políticas de almacenamiento y tareas administrativas que se llevan a cabo:

Hora	L	M	X	J	V	S	D	Política o Programación
08:00	IN	IN	IN	IN	IN	IN	IN	Informe resumen backups
10:00	RD	RD	RD	RD	RD	RD	RD	Backup Recuperación Desastres
12:00	BD	BD	BD	BD	BD	BD	BD	Borrado de datos
17:00	-	-	FTP	-	-	-	-	Descarga de Actualización
10:00		IA						Instalación de Actualizaciones
18:00					C			Backup Completo
12.00	C	C	C	C	C	C	C	Backup BBDDeduplicación
23:59	I	I	I	I	I	I		Backup datos
23:59						SC		Backup datos

IN: Informe resumen
BD: Borrado de datos más antiguos que el ciclo de retención establecido.
FTP: Descarga de actualizaciones
C= Completo
SC: Completo sintético
I: Incremental

Tabla 19: Políticas de programación

Para evitar que las tareas de backups compitan en recursos con las tareas habituales para ofrecer los servicios que realizan las máquinas virtuales, estas se realizan a horas donde el nivel de usuarios a los que se da servicio es mucho menor.

- Librerías de almacenamiento: Las librerías de almacenamiento son las cabinas en las cuales se almacenan las replicas de la información a asegurar. Las librerías utilizadas son una LUN de la cabina principal IBM DS3524 y una cabina del fabricante IMATION, modelo DataGuard T5R, que ya formaba parte del hardware actual de la empresa antes del montaje de la infraestructura virtual y que se reutilizó para estas funciones:
    - LUN de 50 GB, que se utiliza exclusivamente para operaciones de deduplicación. Se mapea a una unidad dentro del servidor físico que actúa como centro de copias de seguridad y se utiliza para el almacenamiento de la base de datos de **deduplicación**, que contiene punteros a los bloques que varían, durante los backup completos, de modo que no se tienen que guardar de nuevo las copias completas, sino que solo almacenamos las diferencias y, de este modo, se optimiza en espacio y en velocidad de

acceso. Se almacena una copia completa y punteros para los datos que se repiten, de modo que no los vuelve a almacenar.

- Cabina IMATION DataGuard T5R, formada por 6 discos de 2 TB en RAID 6 y una capacidad neta aproximada de 9 TB. Esta cabina de almacenamiento está ubicada físicamente en otra sede empresarial, asegurando de este modo la continuidad de negocio en caso de desastre en el CPD donde se aloja el hardware de la infraestructura virtual. En esta librería de almacenamiento, se guardan las copias de seguridad de los objetos del vCenter Server y una copia adicional de la base de datos de recuperación de desastres de Simpana Commvault. La copia principal de la base de datos de recuperación de desastres se realiza en el disco del sistema del servidor físico donde se ha instalado.

La arquitectura de copias de copias de seguridad se muestra en la siguiente figura:

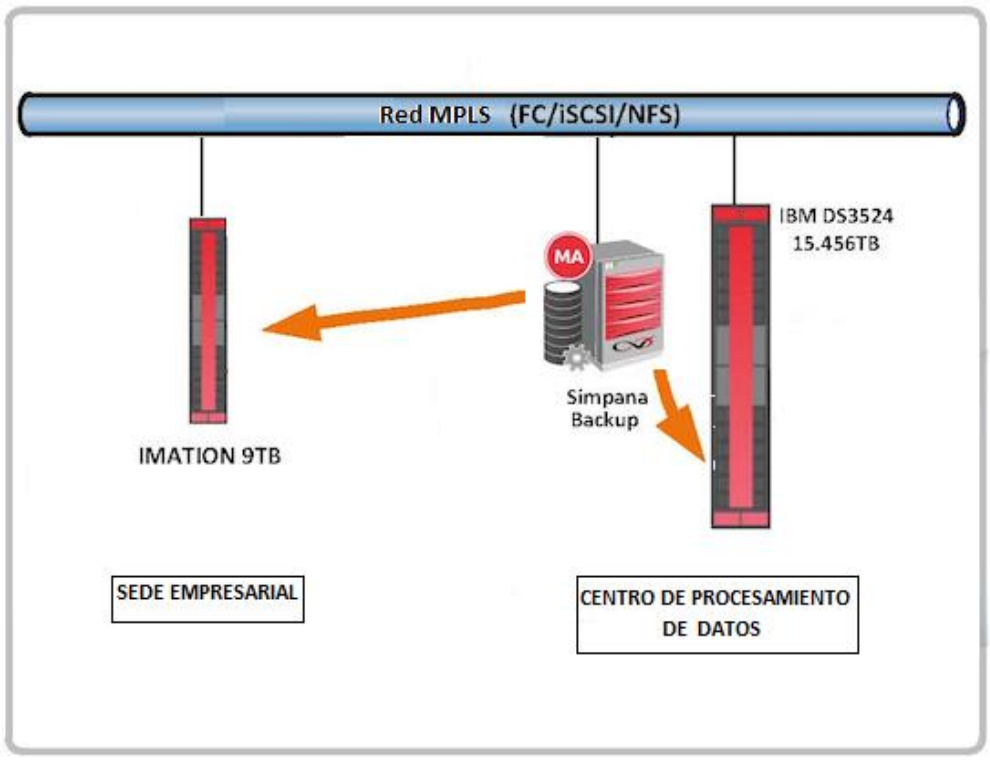


Figura 50: Arquitectura de copias de seguridad

Según la imagen anterior, el software de Simpana realiza la copia de los datos de almacenados en la cabina principal en la cabina IMATION situada en otra sede empresarial. Del mismo modo, realiza una copia de la base de datos de recuperación de desastres desde el disco físico del servidor, Simpana Backup en la imagen, a la cabina IMATION. Por último, se guardan los datos de

deduplicación para el funcionamiento óptimo de la solución Simpana Commvault en una LUN de la cabina principal que se mapea a una unidad de disco del servidor físico.

Las tareas de gestión y administración que se realizan son:

- Realización de backups de máquinas virtuales y plantillas. Inclusión y clasificación de las nuevas máquinas virtuales que se incluyan en las copias de seguridad y eliminación de las máquinas virtuales dadas de baja.
- Programación de informes: se generan informes de funcionamiento diarios que son remitidos por correo electrónico y que ofrecen un resumen de las tareas de backups desarrolladas durante el día anterior y el estado de finalización de dichas tareas. Permiten controlar que todo está funcionando de forma óptima.
- Pruebas de respaldo: recuperación de copias de seguridad. Se realizan pruebas periódicas de recuperación de información para la verificación de que las copias de seguridad se están realizando de forma correcta. Es posible restaurar máquinas virtuales enteras, discos virtuales o archivo individuales. La restauración se realiza por defecto en la misma ubicación que fue origen de la copia pero, si de desea, se puede restaurar con otro nombre, ubicada en otro ESXi o almacenada en otra LUN.

6.2. Replicación del centro de datos

En este apartado se van a describir las herramientas utilizadas para la replicación del centro de datos. Para ello, los elementos principales de la arquitectura de replicación utilizada son una cabina idéntica a la cabina principal, IBM DS3524, y la funcionalidad *Enhanced Remote Mirroring* que pone a disposición el fabricante IBM a través de una licencia Premium [42].

La funcionalidad *Enhanced Remote Mirroring* (ERM) es una característica premium que permite a un sistema de almacenamiento IBM crear una imagen de sus LUN en un otro sistema de almacenamiento compatible y mantener ambas imágenes sincronizadas. ERM es usado para replicación de datos online y en tiempo real entre dos subsistemas de almacenamiento IBM, que deben tener la misma estructura lógica. De esta forma, permite la recuperación de desastres y continuidad de negocio en nuestra compañía ante fallos irrecuperables en la cabina principal. Se puede replicar todas las LUN o unas determinadas, pero siempre es necesario mantener la misma estructura en el subsistema primario y secundario.

De las opciones de funcionamiento disponibles, dentro de la funcionalidad ERM, seleccionamos la denominada *Global mirroring* [42], ya que era la que mejor se adaptaba económica y funcionalmente a nuestras necesidades. Este modo permite mantener una duplicación completa y asíncrona de los datos, permitiendo realizar copias entre CPD separados. *Global Mirroring* puede ser configurado para tener latencias de 3 a 5 segundos con respecto a la E/S del host en la cabina principal. Esta función nos permitirá disponer de una solución de recuperación de desastres de alto rendimiento.

Global mirroring utiliza un modo de escritura asíncrona. Sin embargo, asegura que las solicitudes de escritura se lleven a cabo en el mismo orden en la cabina principal y en la secundaria. Para ello, utiliza un algoritmo de escritura con consistencia en grupo como es mostrado en la siguiente figura:

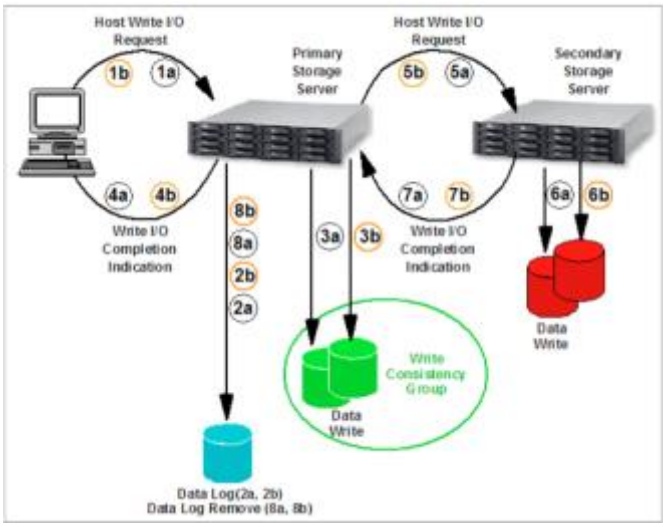


Figura 51: Modo de funcionamiento Global Mirroring (tomada de [42])

Cuando el controlador primario recibe una solicitud de escritura de un host, primero registra la información sobre la escritura en el repositorio secundario en su fichero de *log*. A continuación, escribe los datos en el repositorio local primario. Seguidamente, el controlador inicia la operación de escritura remota para copiar los bloques de datos al repositorio secundario. El orden de la solicitud de escritura en la cabina secundaria se corresponde con el orden de escritura de la cabina principal. Finalmente, borra los datos de registro de la operación.

Para la implementación de la replicación de datos se utilizará, como librería de almacenamiento destino de la sincronización de los datos, una cabina IBM modelo DS3524 idéntica a la principal y situada en un edificio colindante al que aloja nuestro CPD. La solución ideal, que determinan las mejores prácticas, es que la replicación del centro de datos esté al menos a 300 Km del centro de datos principal pero, en nuestro caso, no podíamos abordar dicha condición por razones económicas, logístas e internas de la empresa.

La arquitectura de la red de almacenamiento con la cabina de replicación del centro de datos quedaría como se muestra en la siguiente figura:

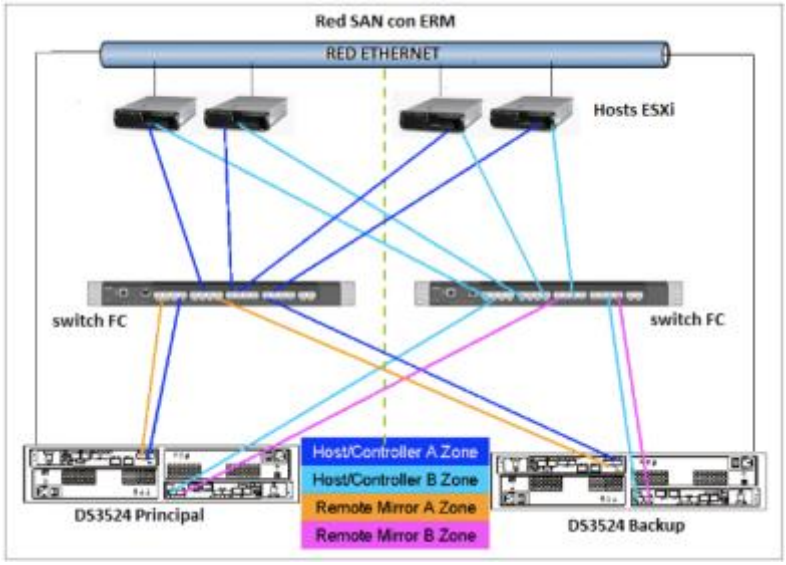


Figura 52: Arquitectura SAN con cabina DS3524 de replicación (tomada de [42])

Como puede observarse en la figura, se ha incluido en la red de almacenamiento de datos la cabina secundaria mediante su conexión a los switches Fiber Channel.

Tras tener definida la arquitectura, se procedió a la instalación de la cabina secundaria y la configuración inicial de la misma siguiendo el mismo procedimiento descrito en el apartado 4.4.2. Para la instalación de la cabina auxiliar son necesarios 4 IBM *SFP Trasceiver 8 Gbps FC SW* para conectar cada una de las controladoras de la cabina auxiliar a ambos switches y 2 IBM *SFP Tranceiver 8 GB FC SW* para instalar en cada una de las controladoras de la cabina auxiliar. Se necesitan además 4 cables de fibra 62.5/125 de 100 metros con conector LC-LC que puso a nuestra disposición la empresa a la que se le tenía contratada el CPD, ya que la ubicación de la cabina secundaria también se contrató a esta empresa. La limitación en distancia para el cableado de la cabina secundaria en esta configuración, utilizando el ERM, era de 500 metros, limitación que cumplíamos ampliamente, ya que la distancia aproximada del cableado de fibra se situaba en torno a los 100m.

Siguiendo la metodología de esta sección, se realizó también el zoning para la inclusión en la red de almacenamiento de esta cabina para la replicación, siguiendo el procedimiento descrito en el capítulo 4.4.1. Los puertos usados por el ERM no pueden ser usados para enviar o recibir datos procedente de cualquier host que accede a la SAN. Este requisito es abordado mediante la definición del zoning SAN. Debe haber dos zonas definidas para la red de ERM, una para el controlador A y una para el controlador B. Cualquier zona definida debe separar los puertos dedicados al almacenamiento de

datos de los hosts y los puertos dedicados al sistema de *mirroring*, y además separar los puertos del mirroring entre controladoras. Cuando se usa ERM, se deben crear dos zonas adicionales:

- La primera zona contine la controladora A de la cabina origen del ERM y la controladora A de la cabina destino del ERM.
- La segunda zona contine la controladora B de la cabina origen del ERM y la controladora B de la cabina destino del ERM.

Una LUN secundaria en un remote mirror siempre tendrá en mismo propietario principal que la LUN primaria asociada. Por ejemplo, si la controladora A posee la LUN primaria en el sistema de almacenamiento principal, la controladora A será propietaria de la LUN secundaria asociada en el sistema de almacenamiento secundario. Si la propiedad del LUN primaria cambia, esto provocará un cambio en la propiedad de la LUN secundaria asociada.

Tras esto, a través del DS Storage Manager se realizaron la activación y configuraciones avanzadas necesarias [42] para el funcionamiento óptimo de la funcionalidad ERM. Finalmente, se llevaron a cabo el banco de pruebas que permitió validar el correcto funcionamiento del sistema de replicación y se puso en marcha el sistema de replicación.

6.3. Protocolo de recuperación de desastres y continuidad de negocio

En este apartado, describiremos brevemente el plan de recuperación de desastres (PRD) y continuidad de negocio que se debe seguir para recuperar la infraestructura virtual. Un plan de recuperación de desastres contiene una serie de procedimientos detallados para recuperar el hardware, el software y los datos en caso de catástrofe, incendio, robo, pérdida de datos masiva, etc., con el fin de restablecer los servicios en el menor tiempo posible y minimizar el impacto. Todo plan integral de recuperación de desastres debe incluir también a todos los proveedores relevantes, las fuentes de experiencia para recuperar los sistemas afectados y una secuencia lógica de los pasos a seguir hasta alcanzar una recuperación óptima.

En el caso de una infraestructura virtual basada en VMware, el fabricante de la tecnología de virtualización ya cuenta con el producto denominado VMware Site Recovery Manager (SRM) que proporciona una recuperación rápida y fiable ante desastres. Se trata de un software para la automatización de la recuperación ante desastres que permite una gestión basada en políticas, la realización de pruebas sin interrupciones y la coordinación automatizada. Sin embargo, este producto se vende con una licencia independiente y su precio se hacía inalcanzable para nuestra compañía. Por ello, hubo que realizar un plan alternativo de elaboración interna para responder ante posibles desastres. Nuestra solución alternativa a SRM es un plan sólido de backup que pueden adaptarse a las necesidades de la empresa y a un precio mucho más accesible.

Lo primero y más importante es identificar los **objetivos** del plan. Para ello, definimos dos valores de tiempo que son los conceptos claves que permiten determinar la excelencia del plan de recuperación de desastres:

- **RPO**: El *Recovery Point Objective* es el punto en el tiempo hasta el cual recuperamos nuestra información, es decir, la cantidad de información que podemos tolerar perder, medido en tiempo, desde el último respaldo disponible o bien desde el último trabajo de replicación realizado exitosamente. A mayor RPO mayor es la pérdida de información**.**
- **RTO**: El *Recovery Time Objective* es el tiempo que tardará la empresa en volver a prestar los servicios con normalidad. A mayor RTO mayor es el tiempo que el servicio permanecerá interrumpido.

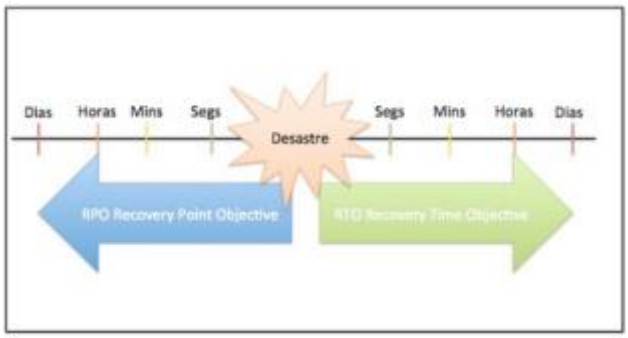


Figura 53: RPO y RTO en un PRD

Los valores de RTO y RPO deben ser aceptados y conocidos por el órgano directivo de la empresa y, dependiendo de la tolerancia de estos valores, se va a seguir uno de los siguientes procedimientos dentro del plan de recuperación de desastres de la arquitectura virtual:

- **Respaldo y recuperación**: Esta basada en una óptima solución de backup a la que habrá que sumar un ambiente virtual donde recuperar los servidores virtuales replicados y luego comenzar a levantar los servicios ordenadamente. Es la solución más sencilla de implementar.
- **Replicación bajo demanda**: Esta alternativa es un poco más costosa pero mas sencilla que la de respaldo y recuperación, pero logra ahorrarnos tener que trabajar con soluciones de backup para la recuperación si podemos tolerar la pérdida de información desde nuestro último trabajo de replicación. En caso de tener que recuperar nuestro ambiente ante un desastre o algún evento que nos impida trabajar en nuestro centro de datos debemos contar con un ambiente virtual donde recuperar nuestros servidores virtuales y luego comenzar a levantar los servicios ordenadamente.
- **Replicación y orquestación**: Esta alternativa se basa en la utilización de VMware Site Recovery Manager proporcionando una recuperación rápida y fiable ante cualquier desastre.

En la siguiente tabla se muestra los valores de RTO/RPO en estos tres escenarios:

	Respaldo y recuperación	Replicación a demanda	VMware SRM
RPO	**Alto**	**Medio**	**Bajo**
RTO	**Alto**	**Bajo**	**Bajo**

Tabla 20: Valores RPO/RTO en un los tres escenarios

Como se desprende de la tabla anterior, la solución más sencilla y económica es la que ofrece peores prestaciones como es lógico. Cabe resaltar que en los dos primeros procedimientos descritos debería existir un procedimiento definido de cómo llevar a cabo el plan de recuperación y, sobre todo, testeado. Sin embargo, cuando se utiliza VMware SRM el proceso es completamente automatizado y ejecutado por el producto.

En nuestro caso, el comité ejecutivo de empresa decidió tolerar valores altos de RTO y RPO, una vez analizada las tres posibles opciones basando su decisión en lo siguiente:

- Razones de presupuesto, entre las que se incluía la limitación de efectivos en el personal del departamento de TI.
- La compañía es una empresa pequeña y no es una empresa de servicios propiamente dicha, sino que su fin principal es otro. Por ello, se podía tolerar la interrupción del servicio en caso de catástrofe o desastre fuerte.

- La compañía prefiere invertir más en disponer de alta disponibilidad y redundancia en la arquitectura virtual antes que "asegurar" la plataforma para una recuperación inmediata ante grandes desastres. La recuperación estaba asegurada, aunque con mayor valor de RTO/RPO.

Por estos motivos, los procedimientos de recuperación de desastres y continuidad de negocio están basados en respaldo y recuperación del centro de datos, que es el mayor activo de la empresa. Cabe resaltar que el procedimiento de recuperación de desastres de la arquitectura virtual puede implementarse de forma mucho más simple que si se dispusiera de una arquitectura física. En una empresa más grande, lo normal es disponer de un Sistema de Gestión de la seguridad de la información (SGSI – ISO 27001) que incluye esta parte del plan de recuperación de desastres y continuidad de negocio. Sin embargo, en nuestra compañía se carece de este plan, pero se decide realizar de forma interna el procedimiento del plan de recuperación de desastres para la infraestructura virtual basada en VMware.

A continuación, vamos a considerar las posibles situaciones adversas que pueden darse en la arquitectura virtual y el procedimiento de recuperación a considerar. Dentro de un SGSI esto se consideraría dentro de Análisis de Riesgos. En nuestro caso vamos a realizar una valoración procedimental considerando los posibles casos de riesgo y teniendo en cuenta los distintos elementos que forman parte de la arquitectura global de la arquitectura virtual:

- Servidores ESXi.

La infraestructura virtual dispone de 6 host ESXi en clúster que, según se ha aprovisionado, podría soportar la caída de uno de los host y seguir funcionando sin interrupción del servicio gracias a vSphere HA. Esto permitiría a la empresa solucionar la avería del hosts sin que el servicio se vea penalizado.

En el caso de que se averiaran de forma simultánea dos ESXi, el servicio vSphere HA podría comenzar a experimentar problemas y habría que asegurarse que las máquinas virtuales que corrían en los ESXi averiados se han migrado sin problemas al resto de host operativos del clúster de forma automática, es decir, que los host restantes tienen recursos suficientes para albergar a las máquinas virtuales que funcionaban en los hosts averiados. Esto dependerá del grado de ocupación de recursos del clúster por parte de las máquinas virtuales. En las pruebas de esfuerzo realizadas después de la instalación de la plataforma, al existir pocas máquinas virtuales la arquitectura virtual asumía sin problemas las caídas de incluso 4 host ESXi. En la actualidad, donde ya existen casi 50 máquinas virtuales, las pruebas de esfuerzo realizadas demuestran que la arquitectura virtual puede soportar la

caída de 2 hosts sin interrupción de servicio, pero el grado de funcionamiento del clúster con los 4 hosts no averiados hace que salten avisos de ocupación de recursos, por lo que ésta situación de funcionamiento solo puede permitirse pocos días.

En el caso de que se averiaran tres, cuatro o cinco servidores ESXi de forma simultánea, el clúster ya no podría sustentar todas las máquinas virtuales que corren con el funcionamiento normal. En este caso, se dejarían encendidas únicamente las máquinas de producción y se apagarían el resto de máquinas. Si fuera necesario, dentro de las máquinas de producción se apagarían máquinas que formen parte de un clúster de servicio y estén redundas, dejando únicamente levantadas las máquinas indispensables para dar servicio. Dependiendo del período de reparación ofrecido por el fabricante (existen contratos de soporte 24x7 de sustitución de servidores incluso) se podrían tomar medidas alternativas como apagar los servicios durante la noche.

En el caso de que se averiara el clúster entero, se produciría la interrupción completa del servicio y la situación sería grave. En este caso, hay que priorizar la subsanación de la avería ESXi a ESXi y una vez dispongamos del primer ESXi recuperado, se levantarán en él las máquinas de producción y a continuación el resto de máquinas según se vayan recuperando el resto de ESXi. De este modo, tratamos de reducir al máximo los parámetros RTO/RPO que es el objetivo de todo plan de recuperación de desastres.

En todas las casuísticas planteadas anteriormente habría que analizar si las averías de los ESXi que se han producido afectan a componentes hardware. Si es el caso, habría que contactar con los fabricantes de los ESXi, en nuestro caso DELL e IBM, para ejecutar el contrato de soporte. En nuestro caso, disponemos de un servicio de soporte que permite la sustitución de cualquier pieza hardware averiada o incluso la sustitución del servidor entero en menos de 24 horas cualquier día del año (servicio 24x7 los 365 días del año), por lo que en este caso el tiempo máximo de restauración del/los servidores ESXi averiados sería de 24 horas para cada servidor ESXi. Es importante elaborar un documento interno con los contactos de los fabricantes y adjuntarlo al procedimiento de recuperación de desastres o de cualquier intervención.

En todos los casos analizados, si la avería en los servidores afectara a los discos del sistema de forma simultánea, para la recuperación del servidor habría que realizar una reinstalación del sistema operativo. En este caso, habría que contactar con el fabricante para que se sustituyeran los discos en el menor tiempo posible. Una vez hecho esto, se debe seguir el procedimiento descrito y documentado que aparece en los apartados 4.3 “Instalación y configuración de los servidores físicos ESXi” y 4.5 “Configuración de la suite VMware vSphere 5” de este documento. En este caso es importante disponer, preparados en todo momento, de un DVD de instalación con el software VMware vSphere 5

Update 1 y una unidad externa USB de DVD. Hay que recordar que los discos del sistema de todos los ESXi disponen de un RAID 1 y, por lo tanto, toleran la avería en uno de los discos siguiendo funcionando sin problemas. En caso de la avería en uno de los discos, habría que adquirir el repuesto para sustituir el disco averiado y, a continuación, agregar el disco al RAID1.

Para hacer un backup de la configuración del host ESXi tras la instalación y tras cambiar la configuración o actualizar el host se utiliza el comando *vicfg-cfgbackup* [3]. Este comando restaura la configuración del host desde la VMware vSphere Command-Line Interface (vCLI). Cuando se realiza un backup de la configuración del ESXi, el número de serie se guarda también en el backup y se restaura junto con esta. En nuestro caso, se conservan backups de la configuración de los ESXi tanto de la configuración inicial como cuando se realiza cualquier actualización.

En el caso de avería más grave, el del clúster de ESXi entero, estimamos que el tiempo máximo para restaurar de nuevo los primeros servicios de producción estaría en torno a 24 horas, pudiendo quedar la plataforma entera restaurada en torno a las 48 horas.

- Vcenter Server

En caso de avería en el servidor físico que incluye la instalación de Vcenter Server, no supondría interrupción del servicio que se proporciona a través de la infraestructura virtual al exterior, pero supondría una interrupción en los servicios internos que ofrece dicho servidor físico dentro de la arquitectura virtual:

- Administración de la plataforma virtual a través del VMware vSphere Client o el VMware vSphere Web Client y todas las funcionalidades de VMware que se realizan a través del vCenter Server: vMotion, vSphere HA, etc.
- Realización de las copias de seguridad a través del Software Simpana Commvault.
- Centro de administración de la cabina de almacenamiento principal.
- Centro de gestión remota de los switches Ethernet y Fiber Channel.
- Centro de descarga de software y realización de instalaciones de nuevas máquinas virtuales.
- Centro de administración y gestión de los ESXi.

Si bien no suponen interrupción del servicio, sí son tareas críticas, sobre todo la realización de las copias de seguridad diarias y, por ello, se debe tratar de solucionar la avería en el menor tiempo posible. Si se trata de una avería hardware, se debe utilizar el contrato de soporte con el fabricante,

DELL en este caso, que permite la sustitución de cualquier hardware averiado en el servidor o incluso el servidor entero en un máximo de 24 horas. Si se trata de un error grave en los discos del sistema o un error software que exige una reinstalación, se debe seguir el procedimiento de instalación en el apartado 4.2 de este documento para restaurar la configuración sobre el vCenter Server. Sin embargo, esta reinstalación no mantendría las configuraciones actuales del servidor ni reflejaría el estado actual del inventario en el vCenter Server. Al guardarse las configuraciones y todos los datos en los discos del sistema del servidor y no en la cabina, es necesaria la realización de copias de seguridad de estos discos para evitar la pérdida de éstas configuraciones y los datos actuales de la plataforma virtual. Por ello, es necesaria la realización de un backup de los discos del sistema de este servidor físico.

Para reducir el tiempo de interrupción del servidor del vCenter Server, se realiza una copia de seguridad del mismo. vCenter Server necesita que se realice un backup de una imagen completa del servidor físico sobre el que funciona. En nuestro caso, la importancia de este backup es todavía mayor debido a las funcionalidades adicionales que tiene este servidor físico dentro de la infraestructura virtual. Por ello, utilizamos el software *Acronis Backup from Windows Server* para realizar un backup completo del servidor físico del vCenter Server que nos permitirá la restauración del mismo en caso de pérdida total de datos de forma más rápida. *Acronis Backup* es una tecnología que permite la creación de imágenes de disco a nivel de bloque que permite capturar todo el servidor Windows Server en un único paso muy sencillo. *Acronis Backup* permite:

- Realizar una copia completa del servidor y la restauración de la misma.
- Recuperar archivos individuales, datos de aplicaciones o un sistema completo.
- Realizar copias de seguridad incrementales y diferenciales, y con compresión. Los procedimientos de instalación y configuración requieren una curva de aprendizaje casi inexistente.
- Restaurar un servidor en un hardware nuevo y distinto, sin preocuparse por las incompatibilidades a nivel hardware.

Con esto conseguimos disponer de una copia completa del vCenter Server que podemos restaurar más rápidamente en caso de catástrofe. A nivel de VMware, los datos y las consideraciones que se deben controlar en el backup de vCenter Server, sobre todo si el backup es manual y selectivo son [43]:

- Hacer un backup sobre su base de datos y de los datos de VMware VCMSDS (Active Directory y Application Mode (ADAM)). Los datos de ADAM se copian cada 5 minutos en la base de datos de vCenter Server dentro del propio funcionamiento de VMware.

- Hacer un backup de los certificados SSL y del archivo vpxd.cfg, que es el servicio principal de Vcenter Server y que se encuentra en el directorio de instalación de vCenter Server dentro del disco del sistema.
- Antes de comenzar los backup deben detenerse los siguientes servicios:
    - VMware Vcenter Server.
    - VMware VCMSDS (base de datos de *Active Directory* y *Application Mode*).
    - El servicio de bases de datos, en nuestro caso SQL.

En cuanto a la restauración del Simpana Commvault, habría que utilizar la base de datos de recuperación de desastres del software de Simpana Commvault para restaurar la instalación y configuración de la consola de gestión de copias de seguridad en este servidor.

- Red Ethernet

La red Ethernet de la infraestructura virtual se encuentra redundada a nivel de switch, de cableado ethernet y de tarjetas de red. Por este motivo, una avería en cualquiera de estos dispositivos hardware de la red no provocaría interrupciones en el servicio. En este caso, si se produjera una avería en cualquier de estos elementos redundados se procedería a su reparación o sustitución si fuera necesario manteniendo la alta disponibilidad. En el caso del cableado Ethernet y las tarjetas de red, se procedería a su sustitución hardware sin más. En cambio, en el caso del switch, se ejecutaría el contrato de soporte para su sustitución o reparación y habría que proceder de nuevo a su instalación y configuración. Para ello, se podría instalar desde cero como se indica en el apartado 4.1 de esta memoria, pero lo más rápido y lógico es hacerlo importando la configuración desde una copia de seguridad de la misma. Para ello, se mantienen copias de seguridad de la configuración inicial de los switches y se realizan nuevas copias cada vez que se modifican las configuraciones o se actualiza el firmware de los mismos.

En el caso de que se produjeran averías en los elementos redundados simultáneamente, se produciría interrupciones de servicio en la plataforma virtual. En el caso del cableado Ethernet y las tarjetas de red, se tendrían que averiar simultáneamente 7 u 8 elementos para que la situación pudiera provocar interrupciones. En este caso, se procedería a su sustitución hardware en el ESXi afectado sin más. Por el contrario, en el caso de los switches, habría que ejecutar los contratos de soporte para su sustitución y reparación y, a continuación, proceder a su configuración mediante la carga de una copia de seguridad de la configuración actual de los mismos antes de la avería. Con este procedimiento se reduciría al máximo el RTO.

- Red SAN
    - Switches Fiber Channel

La red SAN de la infraestructura virtual se encuentra redundada a nivel de switches, cableado y tarjetas HBA. Al encontrarse en un escenario idéntico al de la red ethernet, se seguirían los mismos procedimientos que se han descritos en el apartado anterior pero extrapolados a los switches Fiber Channel, el cableado fiber channel y las tarjetas HBA. En cuanto a los switches Fiber Channel se almacenan copias de seguridad de la configuración inicial de los switches y se realizan nuevas copias cada vez que se modifican las configuraciones o se actualiza el firmware de los mismos.

    - Cabina IBM

Para garantizar la recuperación de desastres y continuidad de negocio del centro de datos se dispone de una replicación del sistema principal de almacenamiento. En caso fallo irrecuperable en la cabina principal se utilizaría esta réplica sincronizada de los datos para permitir la recuperación de los servicios que proporciona la infraestructura virtual. En el caso de catástrofe que afectara al edificio del centro de datos y al colindante que aloja la réplica del centro de datos, se podrían recuperar de nuevo los servicios puesto que se dispone de una copia de los objetos del vCenter Server, aunque existiría algo de pérdida de información, pues solo se recuperaría desde la última copia de datos realizada por el software Simpana Commvault en la cabina IMATION. En este último caso, los valores del RTO y RPO serían mucho más elevados.

6.4. Resumen y conclusiones

En este capítulo se han descrito las políticas y procedimientos llevados a cabo para garantizar la replicación de los datos que permita a la empresa la recuperación de los servicios en caso de catástrofe o fallo grave o parcial en el hardware o software de la arquitectura virtual, garantizando de este modo la continuidad de negocio.

En el primer apartado se ha descrito la arquitectura de copias de seguridad utilizada para disponer de réplicas de los objetos del vCenter Server en una sede remota de la empresa alejada de la sede principal donde se almacena la infraestructura virtual. En el segundo apartado, se ha descrito la arquitectura de replicación del centro de datos que permite disponer de una imagen de la cabina

principal en una ubicación alternativa, garantizando la recuperación ante fallos graves en el centro de datos principal y permitiendo tiempos de recuperación bajos. Finalmente, se han descrito, a alto nivel, los procedimientos que deben realizarse ante fallos irrecuperables de los distintos elementos hardware y software que garantizan el funcionamiento óptimo de la infraestructura virtual y, en consecuencia, los servicios que desde ella se prestan.

Capítulo 7:

7. Conclusiones y líneas futuras

En este capítulo, se van a exponer las conclusiones obtenidas del desarrollo, implantación y administración y gestión de la infraestructura virtual en mi empresa.

Tras finalizar con éxito todas las tareas descritas en esta memoria, se puede afirmar que se ha conseguido el principal objetivo perseguido con este proyecto que no era otro que el diseño e implementación de una arquitectura virtual de servidores. El comienzo de este proyecto se sitúa temporalmente a principios del año 2012 y la implementación de la infraestructura virtual y su puesta en producción finalizó en noviembre de ese mismo año siguiendo las tareas descritas en esta memoria. Desde entonces, todos los servidores necesarios para la implementación de servicios y aplicaciones de la empresa se albergan y funcionan dentro de esta plataforma virtual. El resto de objetivos marcados en la sección 1.2 también se han conseguido con éxito.

Mejoras introducidas con la arquitectura virtual

La implantación de la infraestructura virtual supuso para el departamento TI, del que formo parte, un cambio total en la forma de gestionar los recursos informáticos de la empresa. Todas las ventajas de la virtualización fueron plasmadas en las tareas y procedimientos llevados a cabo a diario. El hecho de cubrir necesidades urgentes de despliegue de servidores, clonar entornos para la realización de pruebas o realización de despliegues son algunas de las tareas que antes suponían verdaderas dificultades por los condicionantes técnicos, económicos o temporales, y ahora se realizan en minutos. Esto ha optimizado los procedimientos tanto internos como externos, y tanto a nivel departamental como a nivel global de la empresa.

El reto de administrar y gestionar la infraestructura se ha conseguido, a parte de la gran formación inicial, gracias a la gran cantidad de blogs de expertos y comunidades de usuarios de VMware que nutren con sus experiencias y resolución de problemas el conocimiento de los administradores de las plataformas virtuales. Además, la experiencia y el conocimiento desarrollado permite optimizar día a día el funcionamiento de todos los elementos que influyen en la arquitectura y permite resolver problemas de forma más eficiente y en tiempos menores.

Desde su implantación, la infraestructura virtual ha ido creciendo en número de máquinas virtuales activas que comparten los recursos que proporciona el clúster de 6 servidores físicos. En la

actualidad, la infraestructura virtual cuenta con 62 máquinas virtuales y sigue funcionamiento de forma óptima. Teniendo en cuenta que durante el diseño se estimó en 40 el número máximo de máquinas virtuales a desplegar, se concluye que el dimensionamiento de recursos de la plataforma virtual fue realizado con acierto. Con estas 62 máquinas virtuales se ha conseguido dar servicio a todos los proyectos planificados al comienzo de la implantación de la arquitectura virtual.

Mejoras introducidas sobre la infraestructura virtual inicial

Del pool de recursos inicial que se desplegó en la infraestructura virtual, el único que se ha considerado aumentar para optimizar el funcionamiento de las aplicaciones ha sido la memoria virtual. Además, la ampliación de este recurso, como ya se vió en el apartado 3.3.3, es relativamente fácil de realizar. Para ello, fueron adquiridos módulos de memoria compatibles y aumentó la memoria hasta el valor máximo que determina la licencia VMware vSphere Standard 5 que, como se calculó en el apartado 3.3.3, se sitúa en 384 GB. Según este valor, se aumentó la memoria RAM de cada uno de los host ESXi desde los 24 GB que disponían inicialmente, hasta los 64 GB como máximo que pueden disponer bajo la licencia vigente de VMware.

La versión de VMware vSphere Standard de la 5.0 Update 1 ha sido actualizada a la versión 5.5. Actualmente, la versión más actual vigente es la versión 6.0, versión a la que se actualizará la plataforma virtual en el próximo año.

Mejoras en el diseño

Tras cuatro años de experiencia en la gestión de la infraestructura virtual desplegada, la única consideración de diseño que modificaría sería sin duda la cabina de almacenamiento. Con un conocimiento mucho más en profundidad el mercado de los fabricantes de las cabinas y las prestaciones que estas consiguen, hubiera tratado de ahorrar algo de costes en otras partidas o incluso cambiar el protocolo de transporte de la red SAN de Fiber Channel a iSCSI, si ello me hubiera proporcionado el ahorro de coste necesario para invertir en una cabina de los fabricantes punteros del mercado. La adquisición de una cabina de mejores prestaciones y la combinación del almacenamiento con memorias SSD aumentaría el rendimiento considerablemente.

Del resto de cosas, solo con un presupuesto muchísimo más elevado se podría aspirar a trabajar con una licencia VMware vSphere Enterprise cuya potencia facilita la optimización del rendimiento de la plataforma.

Acciones futuras

La consolidación y crecimiento de los proyectos actuales, la introducción de nuevos proyectos y la sustitución progresiva de los elementos hardware de la infraestructura virtual, ya amortizada, nos lleva a que se planteen las siguientes acciones a corto plazo sobre la plataforma virtual:

- Introducción de nuevos servidores físicos para añadir al clúster, lo que implica nuevas licencias VMware vSphere para sus procesadores. Además, la adición progresiva de nuevos elementos al clúster facilitará la sustitución de los host ESXi actuales.
- Adquisición de una nueva cabina con elevadas prestaciones y utilización de discos de estado sólido (SSD). Las cabinas actuales serán utilizadas para el almacenamiento de copias de seguridad.
- Adquisición de una licencia *SQL Server Standard* o *Enterprise* para proporcionar mayor capacidad y funcionalidad a la base de datos del inventario de vCenter Server.

La introducción en el mundo de la virtualización me llegó, a nivel laboral, a comienzos del año 2012 y de la mano de VMware. Esta oportunidad me ha permitido conocer en profundidad y trabajar en un mundo apasionante que supone la tecnología del presente y del futuro. Espero seguir adquiriendo conocimiento, experiencia y alguna certificación que me ayude a seguir dedicando parte de mis inquietudes y tareas laborales a la virtualización.

Capítulo 8:

8. Planificación de tareas y Presupuesto

8.1. Planificación de tareas

En esta primera sección se presenta la enumeración cronológica de las distintas tareas llevadas a cabo durante la realización del proyecto. Acompañando a cada tarea, se muestra la estimación de la imputación de horas dedicadas. Estas horas no han sido realizadas de forma continua ya que se han compaginado con otras tareas laborales llevadas a cabo dentro de la empresa.

Tarea	Horas
Análisis y definición de objetivos	90
Planificación y logística	70
Diseño de la arquitectura virtual	190
Instalación y configuración de la infraestructura	150
Configuración avanzada, pruebas de esfuerzo y definición de tareas administración y gestión.	80
Despliegue inicial de servicios	
Elaboración de la memoria del proyecto	190
Cierre del proyecto	5
TOTAL	775

Tabla 21: Tareas del proyecto

Siguiendo la tabla anterior, el número total de horas invertidas en el proyecto asciende a 775 horas. Teniendo en cuenta que un hombre-mes es igual a 131,25 horas(valor típico ofrecido por la UC3M), el número de hombre-mes ascenderá a 775/131,25 = 5,9.

8.2. Presupuesto

El presupuesto final del proyecto es el que se desglosa en las tablas siguientes:

UNIVERSIDAD CARLOS III DE MADRID
Escuela Politécnica Superior

PRESUPUESTO DE PROYECTO

1.- Autor:
Juan José Ávila Lucero
2.- Departamento:
Ingeniería Telemática
3.- Descripción del Proyecto:
- Titulo: Diseño y configuración de una infraestructura virtual con VMware
- Duración (meses): 5,9
Tasa de costes Indirectos: 20%

4.- Presupuesto total del Proyecto (valores en Euros):
Euros

5.- Desglose presupuestario (costes directos)

PERSONAL

Apellidos y nombre	N.I.F. (no rellenar - solo a titulo informativo)	Categoría	Dedicación (hombres mes) [a]	Coste hombre mes	Coste (Euro)	Firma de conformidad
Juan José Ávila Lucero		Ingeniero	5,9	2.694,39	0,00	
					0,00	
					15.896,90	
					0,00	
					0,00	
		Hombres mes	**5,9**	**Total**	15.896,90	

[a] 1 Hombre mes = 131,25 horas. Máximo anual de dedicación de 12 hombres mes (1575 horas)
Máximo anual para PDI de la Universidad Carlos III de Madrid de 8,8 hombres mes (1.155 horas)

EQUIPOS

Descripción	Coste (Euro)	% Uso dedicado proyecto	Dedicación (meses)	Periodo de depreciación	Coste imputable [c]
Servidor IBM X3550 M3	3.419,06	100	60	60	3.419,06
Servidor IBM X3550 M3	3.419,06	100	60	60	3.419,06
Servidor IBM X3550 M3	3.419,06	100	60	60	3.419,06
Servidor Dell PowerEdge R410	2.846,30	100	60	60	2.846,30
Servidor Dell PowerEdge R410	2.846,30	100	60	60	2.846,30
Cabina DS3524	5.214,24	100	60	60	5.214,24
Cabina DS3524	5.214,24	100	60	60	5.214,24
Switch FC Express IBM SAN24B-4	4.459,13	100	60	60	4.459,13
Switch FC Express IBM SAN24B-4	4.459,13	100	60	60	4.459,13
Switch Ethernet AT/8000GS	989,50	100	60	60	989,50
Switch Ethernet AT/8000GS	989,50	100	60	60	989,50
Cables FC 5 metros LC-LC	658,08	100	60	60	658,08
Cables Ethernet 3 metros Cat6	260,26	100	60	60	260,26
Licencias Vmware Vsphere 5	14.565,06	100	60	60	14.565,06
					0,00
					0,00
				Total	52.758,92

[c] Fórmula de cálculo de la Amortización:

$$\frac{A}{B} x C x D$$

A = nº de meses desde la fecha de facturación en que el equipo es utilizado
B = periodo de depreciación (60 meses)
C = coste del equipo (sin IVA)
D = % del uso que se dedica al proyecto (habitualmente 100%)

SUBCONTRATACIÓN DE TAREAS

Descripción	Empresa	Coste imputable
Instalación/configuración Licencias		
Backup Simpana Commvauilt	EMPRESA 2	2.900,00
	Total	2.900,00

OTROS COSTES DIRECTOS DEL PROYECTO[e)]

Descripción	Empresa	Costes imputable
Material de Oficina		150,00
Dietas		350,00
	Total	500,00

[e)] Este capítulo de gastos incluye todos los gastos no contemplados en los conceptos anteriores, por ejemplo: fungible, viajes y dietas, otros,...

6.- Resumen de costes

Presupuesto Costes Totales	**Presupuesto Costes Totales**
Personal	15.897
Amortización	52.759
Subcontratación de tareas	2.900
Costes de funcionamiento	500
Costes Indirectos	14.411
Total	86.467

Tabla 22: Presupuesto final del proyecto

Capítulo 9:

9. Glosario de acrónimos y abreviaturas:

A continuación, se muestra la relación de los principales acrónimos y abreviaturas que aparecen a lo largo de esta memoria con sus significados correspondientes.

Auto Deploy: Sistema que permite un despliegue automático de uno o varios Hosts a través de la red.

Ballooning: Método de reutilización de recursos de Memoria RAM entre Maquinas Virtuales de un mismo Host.

Cisco Nexus: Switch virtual distribuido de Cisco que incrementa las características y se integra con los switches físicos de Cisco.

Clon: copia exacta de una Maquina Virtual

Clúster: Conjunto de dos o más Hosts para aprovisionar de sistemas de Alta Disponibilidad, Tolerancia a Fallos, Asignación de Recursos y Ahorro de Energía.

Core: número de núcleos del que dispone un Procesador. Los procesadores pueden ser de 2, 4, 6, 8 o más núcleos. A mayor cantidad de cores/núcleos, mayor capacidad de procesamiento dispondremos.

CPU Scheduler: aprovisiona recursos de CPU a los diferentes Worlds asignándolos a los diferentes CPUs del Procesador Físico. Asigna (y balancea) vCPUs a CPUs físicas.

Datastore: Espacio de almacenamiento de un Host de VMware para almacenar Maquinas Virtuales, Plantillas y/o Ficheros ISOs. Pueden tener formato NFS o VMFS.

DCUI: Consola de gestión del Host ESXi. Es lo que se ve si conectamos un monitor al Host físico o si nos conectamos con un sistema tipo iLO, CMC o iDRAC.

Distributed Power Management (DPM): Sistema de ahorro de energía que migra las Maquinas

Virtuales a otros Hosts y apaga el Host físico para ahorrar energía. Cuando el Cluster necesita más recursos se enciende automáticamente el Hosts y se vuelven a migrar las Maquinas Virtuales.

Distributed Resource Scheduler (DRS): Sistema de distribución manual, semiautomatic y automatic de Maquinas Virtuales entre dos o más Hosts con el fin de conseguir un mejor aprovechamiento de los recursos.
Fault Tolerance (FT): Método de tolerancia a fallos de Maquinas Virtuales. Es semejante a un RAID 1 de discos, pero a nivel de Maquina Virtual.

HBA (Hot Bus Adapter) es una tarjeta hardware que se instala en un equipo (servidor) normalmente en el puerto SCSI y permite conectar mediante Fiber Channel (canal de fibra) el equipo con un sistema de almacenamiento en fibra (SAN).

High Availability HA: Sistema de Alta Disponibilidad que permite encender de forma automática una Maquina Virtual en caso de caída de un Host.

Host: Servidor físico que ejecuta un Hipervisor. En el caso de utilizar la tecnología de virtualización VMware se le denomina ESX o ESXi(a partir de la versión 5 de VMware vSphere).

Host Profile: tecnología que permite copiar y distribuir las preferencias de maquetación de un Host e importarlo en otros Host. Este sistema permite ahorrar tiempo de despliegue de Hosts en entornos medianos y grandes.

Hot Add: Método de VMware que permite añadir hardware en caliente como CPU y Memoria RAM. Está limitado tanto por la licencia de vSphere como también por la versión de Sistema Operativo.

HyperThreading: tecnología propietaria de Intel que permite optimizar el uso de los Procesadores pudiendo utilizar múltiples procesos de forma paralela.

IOPS: Operaciones de entrada/salida por segundo a un sistema de almacenamiento. Estará limitado tanto por el tipo de disco y sistema RAID a utilizar.

iSCSI: protocolo de acceso al almacenamiento de Red con tecnología Ethernet.

Latencia: tiempo de espera desde que un sistema hace una petición (Host) hasta que el destino lo responde (SAN).

Linked Mode: sistema de conexión entre un servidor de vCenter y otro permitiendo acceder al inventario global de forma centralizada.

Lock Down: método de seguridad que obliga a un cliente de vSphere gestionar un Host de vSphere siempre a través de un servidor de vCenter.

LUN: espacio de disco en bruto (sin formato) que presenta un sistema de almacenamiento (SAN) a uno o varios Hosts.

NFS: sistema de ficheros que presenta un dispositivo o servidor y lo presenta a uno o varios Hosts.

NIC TEAM: conjunto de una o más tarjetas de red físicas (NIC) que trabajan en conjunto para aportar alta disponibilidad y balanceo de carga a un Host.

Plantilla: formato de Maquina Virtual que permite ser clonada y personalizada. Únicamente está soportada en vCenter Server

Plugin vCenter: aplicación que se integra con la consola de gestión del servidor de vCenter Server.

Pool: un conjunto de recursos de CPU y memoria procedentes de un host ESXi o un clúster.

Pool Automático: objeto lógico de VMware View que permite un despliegue automático de Maquinas Virtuales (Escritorios). El despliegue se hace desde plantillas de vCenter.

Pool de Recursos: sistema que permite reservar y asignar recursos a una o más Maquinas Virtuales.

Pool Manual: objeto lógico de VMware View que presenta una o varias Maquinas Virtuales (Escritorios). Las Maquinas Virtuales tienen que estar previamente desplegadas.

Port Group: objeto lógico que aporta funcionalidad a un switch virtual. Existen dos clases de Port Groups. Virtual Machine y VMkernel (vMotion – iSCSI – FT - Management).

PowerCLI: sistema de automatización de tareas con scripts de PowerShell.

Procesador o Socket: Procesador del Host físico. Un Procesador cuenta con Cores, Caché y GHz entre las características más importantes.

Replicación: método de copia de una Maquina Virtual desde un Host a otro y desde un Datastore a otro con el fin de recuperar una VM de forma inmediata. Existen sistemas de réplicas por Software y por Hardware (desde una SAN a otra).

Storage vMotion: operación que mueve en caliente los ficheros de una Maquina Virtual desde un Datastore a otro. La Maquina Virtual continúa ejecutándose en el mismo Host.

Target: servidor iSCSI. Dirección IP a la que se apunta con el protocolo iSCSI para conectar al almacenamiento.

ThinAPP: tecnología que permite la virtualización de Software.

VAAI: tecnología de almacenamiento en la cual el sistema de almacenamiento realiza tareas que normalmente las realiza el Host como pueden ser Clonado, Inicialización de discos Thick y Despliegue de Plantillas.

VASA: sistema que permite gestionar y obtener una mayor información de un sistema de almacenamiento.

vCenter Data Recovery: Virtual Appliance de VMware para realizar Copias de Seguridad en caliente de Maquinas Virtuales.

vCenter Update Manager: sistema de VMware que permite actualizar los Hosts, instalar Parches y Actualizaciones (similar al Microsoft WSUS).

vCenter Server: servidor de VMware que gestiona de forma centralizada todos los Hosts y sus recursos. Existen tecnologías como vMotion, svMotion, HA, FT, DRS y demás que únicamente funcionan sobre un vCenter Server.

vdSwitch (Switch Virtual Distribuido): switch virtual que se crea a nivel de vCenter y permite gestionar NICs y Port Groups de uno o más Hosts físicos.

Virtual Appliance: Maquina Virtual que se descarga y se importa al inventario. Suelen ser maquinas empaquetadas listas para utilizar.

vCenter Converter: software que permite conversiones P2V (Físico a Virtual) y V2V (Virtual a Virtual). Se trata de una herramienta gratuita de VMware.

VMFS: sistema de ficheros de VMware que permite un acceso compartido por varios Hosts.
vMotion: tecnología que permite mover una Maquina Virtual en caliente (sin necesidad de apagarla) de un Host a otro.

vShield: suite de productos de seguridad de VMware. Entre ellos están vShield EndPoint, vShield App, vShield Edge y vShield Manager.
vSphere Client: software de Windows que permite gestionar un Host de vSphere (ESXi) o una instancia de vCenter Server.

vSphere Web Client: versión de vSphere Cliente sobre Web.

vSwitch (Switch Virtual): switch virtual que permite gestionar NICs y Port Groups de un Host.

Capítulo 10:

10. Bibliografía y referencias

[1]. VMware Education Services: *VMware vSphere: Instalación, Configuración y gestión Volumen I. ESXi 5.1 y Vcenter Server 5.1*. VMware Inc. 2012.

[2] José María González. *Descubre y domina VMware vSphere™ 5*. Segunda Edición JmG Virtual Consulting, S.L. 2013.

[3] Scoot Lowe. *Mastering VMware vSphere 5*. Wiley, Octubre 2011.

[4] *Comparison Guide VMware vSphere vs Hyper-V y Xen Server 5.6*. http://www.VMware.com/files/pdf/VMware-vsphere-features-comparison-ch-en.pdf

[5] VMware: *VMware y la revolución del cloud computing: un enfoque progresivo*. VMware Inc. 2010.

[6] *VMware: VMware vSphere edición estándar: Hoja de datos.* http://myslide.es/documents/datasheet-vsphere-5-standard-edition-in-spanish.html

[7] *VMware Capacity Planner Datasheet*. http://www.VMware.com/files/pdf/datasheet_capacity_planner.pdf

[8] VMware. *VMware Vsphere 5.0: Licencias, precio y paquetes. Documento técnico*. VMware Inc. 2012

[9] *VMware. Performance Best Practices for VMware vSphere™ 5.0.* http://www.VMware.com/pdf/Perf_Best_Practices_vSphere5.0.pdf

[10] *DELL Power Edge R410*. http://www.dell.com/downloads/emea/products/R410_spec_sheet.pdf

[11] *IBM System x3550 M3*. http://content.etilize.com/user-manual/1019391259.pdf

[12] *Servidores Power Egde: Memoria.* http://www.dell.com/downloads/global/products/pedge/es/11G_DDR3_Memory.pdf

[13] *Configurar y administrar VLAN*. http://www.wetcom.com/content/entendiendo-el-uso-de-vlans-en-VMware/

[14] *Switch AT8000GS/48*. http://www.alliedtelesis.com/documents/8000gs-series-web-guide

[15] *Sistemas avanzados de almacenamiento RAID, NAS y SAN*. https://oposcaib.wikispaces.com/file/view/Tema+4+-+Almacenamiento+avanzado.pdf

[16] *iSCSi vs Fiber Channel explained*. http://www.cuttedge.com/files/iscsi_vs_fiberchannel_explain.pdf

[17] *iSCSi frente a Fiber Channel*.
http://www.techweek.es/empresas/tech-labs/1000016002701/iscsi-frentre-fibre-channel.1.html

[18] IBM Corporation. *IBM System Storage DS3500 and EXP3500 Storage. Subsystem. Installation, User's, and Maintenance Guide*. IBM Corporation 2010, 2013

[19] IBM Corporation. *IBM System Storage DS3524 Express DC and EXP3524 Express DC models are designed for telecommunications and service provider environments*. IBM United States Hardware Announcement February 15, 2011

[20] *IBM System Storage SAN24B-4 Express*.
http://www-03.ibm.com/systems/es/storage/san/b-type/san24b-4/

[21] *QLogic 8Gb FC Single-port and Dual-port HBAs for System x*.
https://lenovopress.com/tips0721-qlogic-8gb-fc-hba

[22] Allied Telesis. *AT-8000GS Series Stackable Gigabit Ethernet Switches Installation Guide*. 613-000974 Rev. D Allied Telesis, Inc. 2010.

[23] Allied Telesis. *Command Line Interface User's Guide Allied Telesis AT-8000S*. Allied Telesis, Inc. 2011.

[24] *VMware Knowledge Base. Ejemplo de configuración para el etiquetado VLAN del conmutador virtual (modo VST) (2033047)*
https://kb.VMware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&extern a lId=2033047

[25] VMware: *Prácticas recomendadas para la instalación de vCenter Server 5.0 (2033149).* VMware Knowledge Base 2011.

[26] *Sistemas Dell™ PowerEdge™ R410 Manual del propietario del hardware*. *Dell Inc. Abril 2011*

[27] *Información de System[X]. Servidores de bastidores: IBM System x3550 M3*.
http://publib.boulder.ibm.com/infocenter/systemx/documentation/index.jsp?topic=

[28] VMware: *vSphere Installation and Setup: vSphere 5.0, ESXi 5.0, vCenter Server 5.0*. VMware Inc. 2011.

[29] IBM: *SAN24B-4 Express Installation, Service, and User Guide*. IBM Corporation 2008.

[30] *Brocade EZSwitchSetup Administrator's Guide*.
http://www.brocade.com/content/html/en/administration-guide/fos-741-ezswitchsetup/GUID-73684849-C02D-445E-B7D2-CC0C9D2D0D98.html

[31] *IBM Corporation. Advanced Web Tools Administrator's Guide. IBM Corporation 2010*
http://instrumentation.obs.carnegiescience.edu/FourStar/Documents/FourStar%20Commercial%20M

nuals/Brocade%20SAN%20Switch/software/53_0000522_07.pdf

[32] *Brocade White Paper: Secure SAN Zoning Best Practices.* https://community.brocade.com/dtscp75322/attachments/dtscp75322/fibre/3133/1/Secure+SAN+Zoning+Best+Practices+White+Paper.pdf

[33] IBM: *IBM System Storage DS3500 - Guía de inicio rápido e instalación en bastidor*. IBM Corporation 2010.

[34] IBM Redbooks: *IBM System Storage DS3500 Introduction and Implementation Guide*. IBM Corporation 2011.

[35] IBM: *IBM System Storage DS Storage Manager Version 10 Installation and Host Support Guide*. IBM Corporation 2013.

[36] VMware: *vCenter Server and Host Management Guide 5.1*. VMware Inc. 2009.

[37] VMware Education Services: *VMware vSphere: Instalación, Configuración y gestión Volumen II. ESXi 5.1 y Vcenter Server 5.1*. VMware Inc. 2012.

[38] VMware: *VMware vCenter Converter Standalone User's Guide*. VMware Inc. 2008-2013.

[39] VMware Education Services: *VMware vSphere: Optimize and Scale Volumen I. ESXi 5.1 y Vcenter Server 5.1*. VMware Inc. 2012.

[40] VMware Education Services: *VMware vSphere: Optimize and Scale Volumen II. ESXi 5.1 y Vcenter Server 5.1*. VMware Inc. 2012.

[41] Commvault Documentation versión 10. *https://documentation.commvault.com/commvault/v10/article*

[42] IBM System Storage DS Storage Manager Copy Services Guide. *http://www.redbooks.ibm.com/redbooks/pdfs/sg247822.pdf*

[43] Backing up and restoring vCenter Server 4.x and 5.0 (1023985). *http://www.VMware.com/kb/1023985*

Otras referencias de interés:

Comunidades de VMware: http://communities.VMware.com

Soporte de VMware: http://www.VMware.com/support

Formación de VMware: http://www.VMware.com/education

VMware vSphere Documentation: http://www.VMware.com/support/pubs/vSphere-esxi-vcenter-server-pubs.html